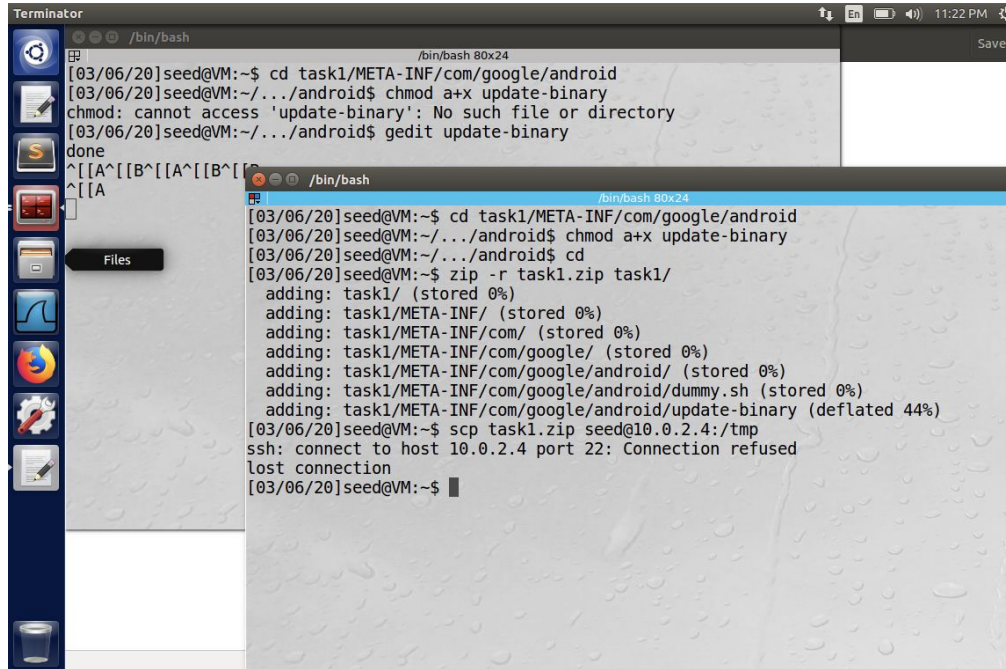


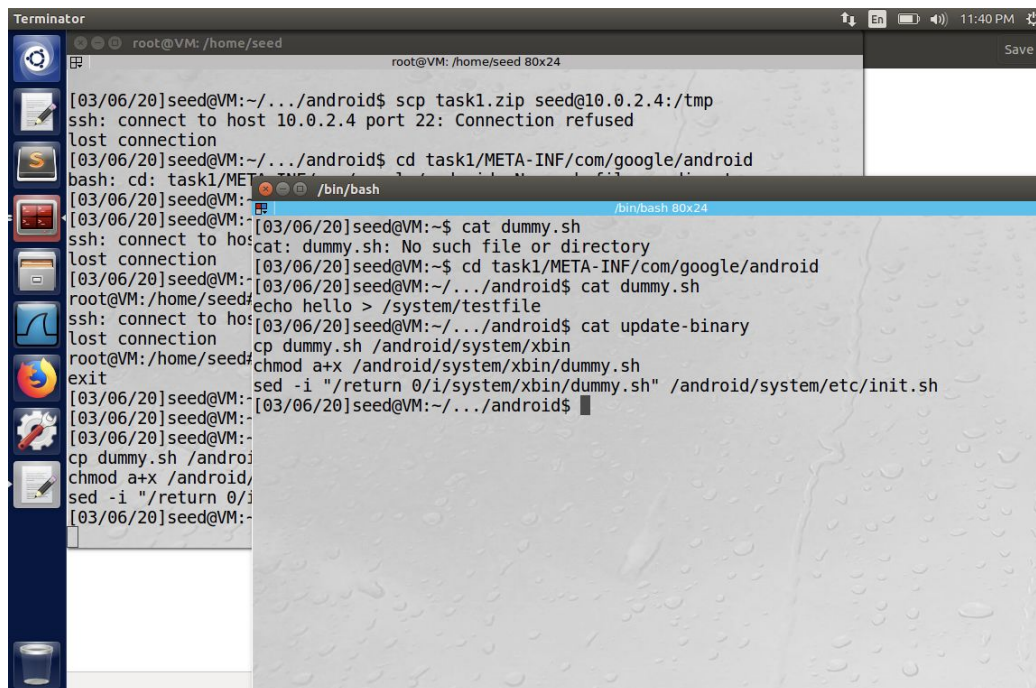
Lab 9
Karsen Diepholz
6 March 2020

Task 1



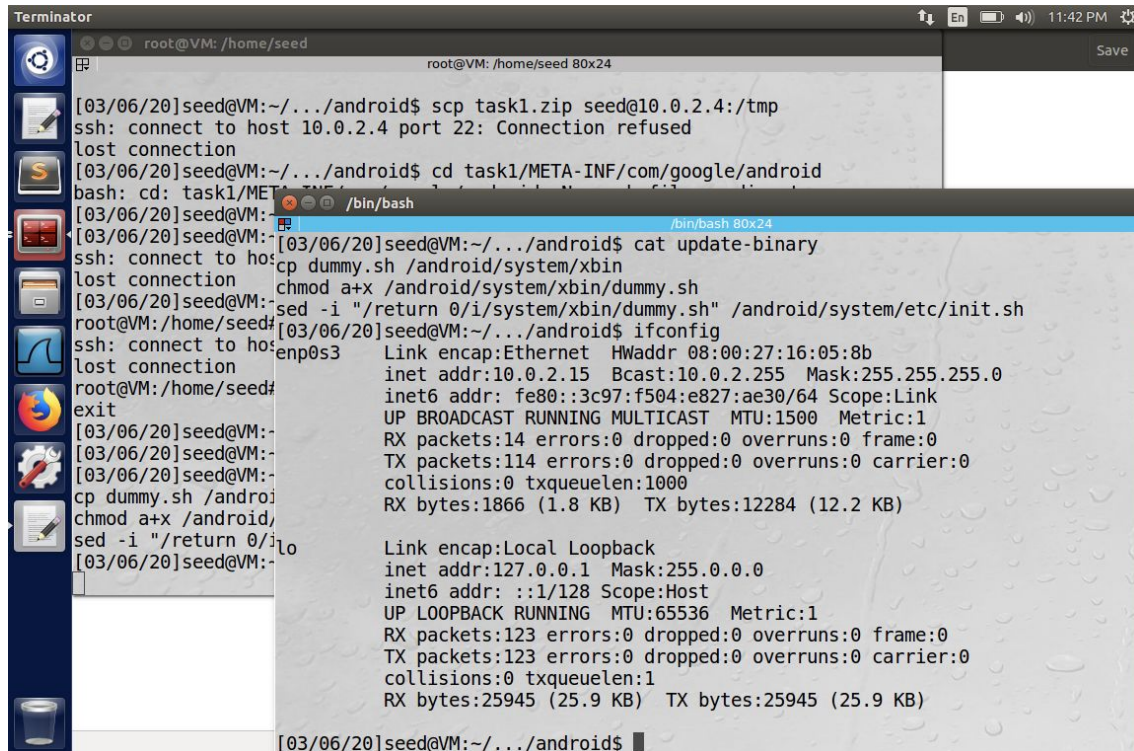
```
Terminator
[03/06/20]seed@VM:~$ cd task1/META-INF/com/google/android
[03/06/20]seed@VM:~/.../android$ chmod a+x update-binary
chmod: cannot access 'update-binary': No such file or directory
[03/06/20]seed@VM:~/.../android$ gedit update-binary
done
^[[A^[[B^[[A^[[B^[[
^[[A
Files
[03/06/20]seed@VM:~$ cd task1/META-INF/com/google/android
[03/06/20]seed@VM:~/.../android$ chmod a+x update-binary
[03/06/20]seed@VM:~/.../android$ cd
[03/06/20]seed@VM:~$ zip -r task1.zip task1/
adding: task1/ (stored 0%)
adding: task1/META-INF/ (stored 0%)
adding: task1/META-INF/com/ (stored 0%)
adding: task1/META-INF/com/google/ (stored 0%)
adding: task1/META-INF/com/google/android/ (stored 0%)
adding: task1/META-INF/com/google/android/dummy.sh (stored 0%)
adding: task1/META-INF/com/google/android/update-binary (deflated 44%)
[03/06/20]seed@VM:~$ scp task1.zip seed@10.0.2.4:/tmp
ssh: connect to host 10.0.2.4 port 22: Connection refused
lost connection
[03/06/20]seed@VM:~$
```

This shows me zipping the contents of task1 into a folder and sending them to the host (android) machine



```
Terminator
root@VM: /home/seed
[03/06/20]seed@VM:~/.../android$ scp task1.zip seed@10.0.2.4:/tmp
ssh: connect to host 10.0.2.4 port 22: Connection refused
lost connection
[03/06/20]seed@VM:~/.../android$ cd task1/META-INF/com/google/android
bash: cd: task1/META-INF/com/google/android: No such file or directory
[03/06/20]seed@VM:~$ /bin/bash
[03/06/20]seed@VM:~$ cat dummy.sh
cat: dummy.sh: No such file or directory
[03/06/20]seed@VM:~$ cd task1/META-INF/com/google/android
[03/06/20]seed@VM:~/.../android$ cat dummy.sh
root@VM:/home/seed$ echo hello > /system/testfile
ssh: connect to host 10.0.2.4 port 22: Connection refused
lost connection
root@VM:/home/seed$ cp dummy.sh /android/system/xbin
exit
[03/06/20]seed@VM:~$ chmod a+x /android/system/xbin/dummy.sh
sed -i "/return 0/i/system/xbin/dummy.sh" /android/system/etc/init.sh
[03/06/20]seed@VM:~/.../android$
[03/06/20]seed@VM:~$ cp dummy.sh /android/system/xbin
[03/06/20]seed@VM:~$ chmod a+x /android/system/xbin/dummy.sh
[03/06/20]seed@VM:~$ sed -i "/return 0/i/system/xbin/dummy.sh" /android/system/etc/init.sh
[03/06/20]seed@VM:~$
```

Using cat, we can see the contents of dummy.sh and update-binary in which i sent to the android VM



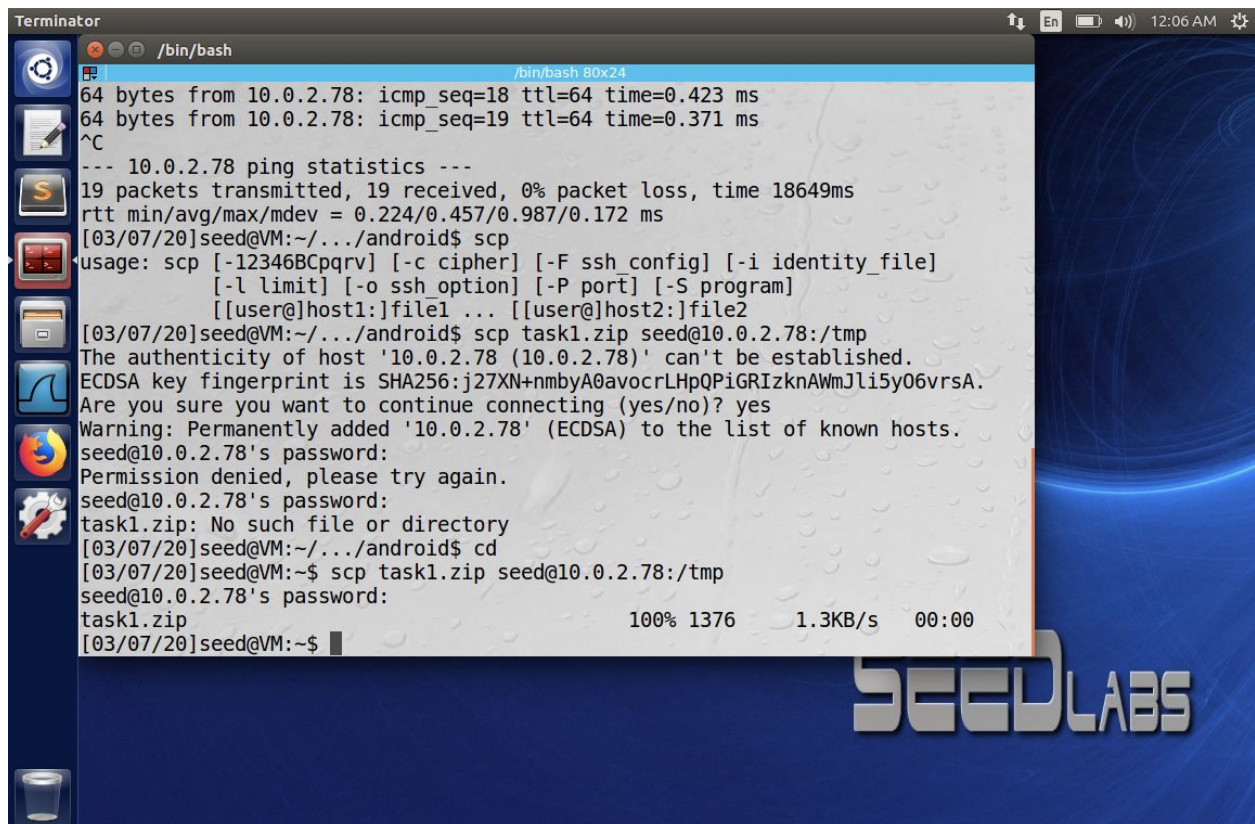
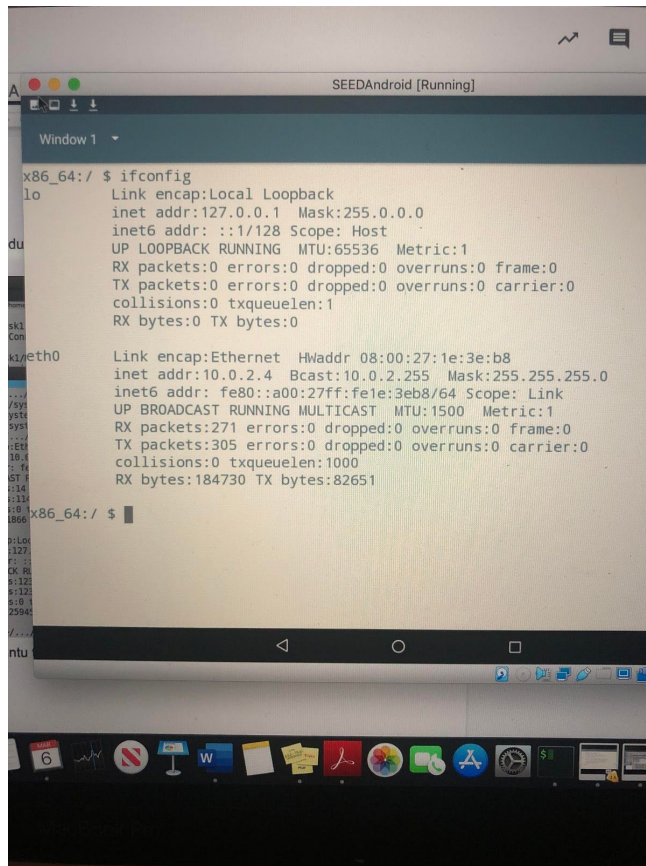
```
Terminator
root@VM: /home/seed
root@VM: /home/seed 80x24
Save

[03/06/20]seed@VM:~/../android$ scp task1.zip seed@10.0.2.4:/tmp
ssh: connect to host 10.0.2.4 port 22: Connection refused
lost connection
[03/06/20]seed@VM:~/../android$ cd task1/META-INF/com/google/android
bash: cd: task1/META-INF/com/google/android: No such file or directory
[03/06/20]seed@VM:~/../android$ /bin/bash
[03/06/20]seed@VM:~/../android$ cat update-binary
cp dummy.sh /android/system/xbin
chmod a+x /android/system/xbin/dummy.sh
sed -i "/return 0/i/system/xbin/dummy.sh" /android/system/etc/init.sh
[03/06/20]seed@VM:~/../android$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:16:05:8b
            inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: fe80::3c97:f504:e827:ae30/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:14 errors:0 dropped:0 overruns:0 frame:0
            TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1866 (1.8 KB)  TX bytes:12284 (12.2 KB)

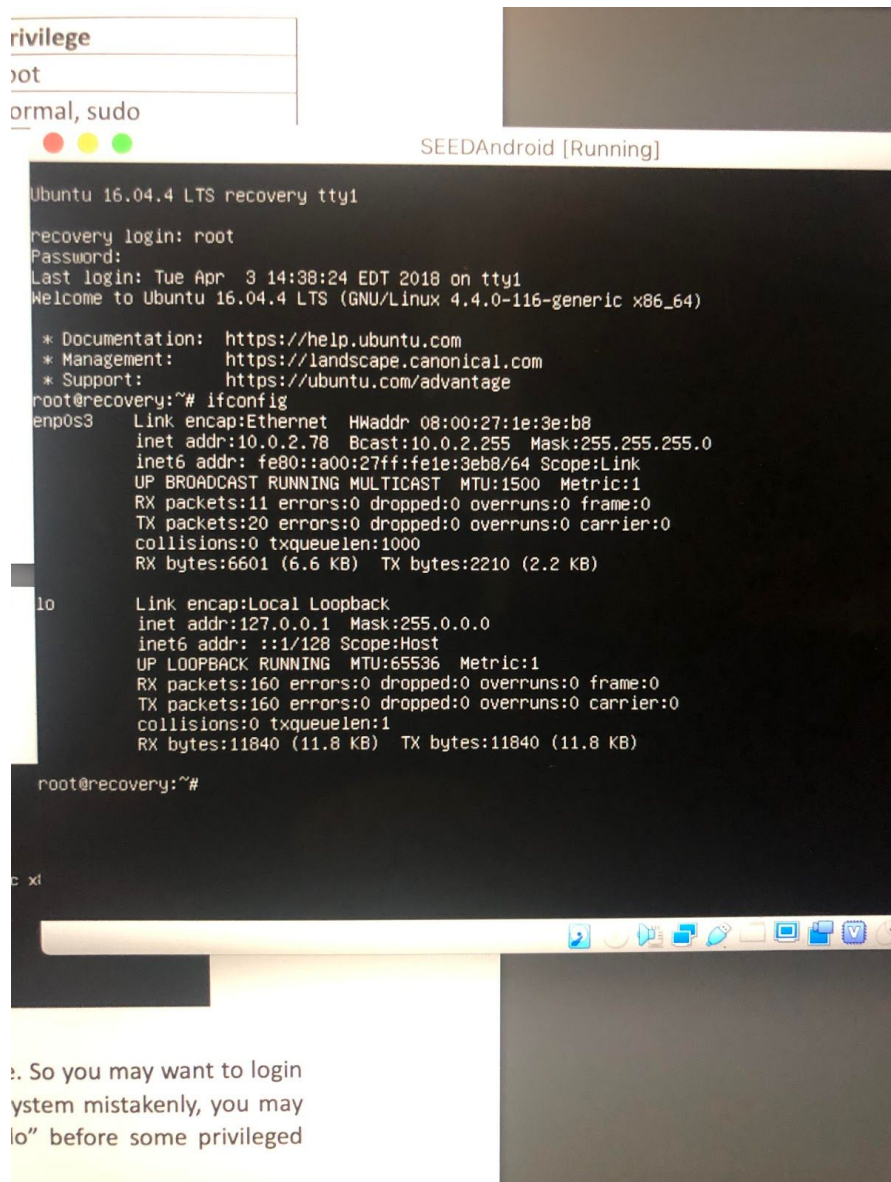
            Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:123 errors:0 dropped:0 overruns:0 frame:0
            TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:25945 (25.9 KB)  TX bytes:25945 (25.9 KB)

[03/06/20]seed@VM:~/../android$
```

We are able to see the IP of our Ubuntu through this command



I successfully transferred the file using the android IP: 10.0.2.78




```
sa:ae:03:dd:b3:8a:3
SEEDAndroid [Running]
)? file1.zip1 may be a wildcard. -Z => ZipInfo mode ("unzip -Z" for usage).
1
-p extract files to pipe, no messages      -l list files (short format)
-f freshen existing files, create none     -t test compressed archive data
-u update files, create if necessary        -z display archive comment only
-v list verbosely/show version info       -T timestamp archive to latest
4 -x exclude files that follow (in xlist)  -d extract files into exdir

modifiers:
-n never overwrite existing files          -q quiet mode (-qq => quieter)
-o overwrite files WITHOUT prompting       -a auto-convert any text files
-j junk paths (do not make directories)    -aa treat ALL files as text
-U use escapes for all non-ASCII Unicode   -UU ignore any Unicode fields
-C match filenames case-insensitively     -L make (some) names lowercase
-X restore UID/GID info                   -U retain UMS version numbers
-K keep setuid/setgid/tacky permissions   -M pipe through "more" pager
-O CHARSET specify a character encoding for DOS, Windows and OS/2 archives
-I CHARSET specify a character encoding for UNIX and other archives

See "unzip -hh" or unzip.txt for more help. Examples:
unzip data1 -x joe => extract all files except joe from zipfile data1.zip
unzip -p foo | more => send contents of foo.zip via pipe into program more
unzip -fo foo ReadMe => quietly replace existing ReadMe if archive file newer

seed@recovery:/tmp$ unzip task1.zip
Archive: task1.zip
creating: task1/
creating: task1/META-INF/
creating: task1/META-INF/com/
creating: task1/META-INF/com/google/
creating: task1/META-INF/com/google/android/
extracting: task1/META-INF/com/google/android/dummy.sh
inflating: task1/META-INF/com/google/android/update-binary
seed@recovery:/tmp$ cd task1/META-INF/com/google/android
dr0seed@recovery:/tmp/task1/META-INF/com/google/android$ ls -l
total 4
-rw-rw-r-- 1 seed seed  0 Mar  6 23:18 dummy.sh
-rwxrwxr-x 1 seed seed 143 Mar  6 23:19 update-binary
binseed@recovery:/tmp/task1/META-INF/com/google/android$ _

Send the Alt Print Screen sequence to the virtual m
droid$ _

and run the update-binary script.
```

Successful unzip of task1 into the android VM

Task 2

Showing my processes...

Terminator

Open ▾ | Save

app_process.c x compile.sh x Application.mk x Android.mk x

```
LOCAL_PATH := $(call my-dir)
include $(CLEAR_VARS)
LOCAL_MODULE := app_process
LOCAL_SRC_FILES := app_process.c
include $(BUILD_EXECUTABLE)
```

/bin/bash

```
[03/07/20]seed@VM:~/.../android$ cat app_process.c
# include <stdio.h>
# include <stdlib.h>
# include <unistd.h>

extern char ** environ;

int main(int argc, char ** argv) {
    // Write the dummy file
    FILE * f = fopen("/system/dummy2", "w");
    if (f == NULL) {
        printf("Permission Denied.\n");
        exit(EXIT_FAILURE);
    }
    fclose(f);

    // Launch the original binary
    char * cmd = "/system/bin/app_process_original";
    execve(cmd, argv, environ);

    // execve () returns only if it fails
    return EXIT_FAILURE;
}
```

[03/07/20]seed@VM:~/.../android\$

Terminator

Open ▾ | Save

app_process.c x compile.sh x Application.mk x Android.mk x

```
LOCAL_PATH := $(call my-dir)
include $(CLEAR_VARS)
LOCAL_MODULE := app_process
LOCAL_SRC_FILES := app_process.c
include $(BUILD_EXECUTABLE)
```

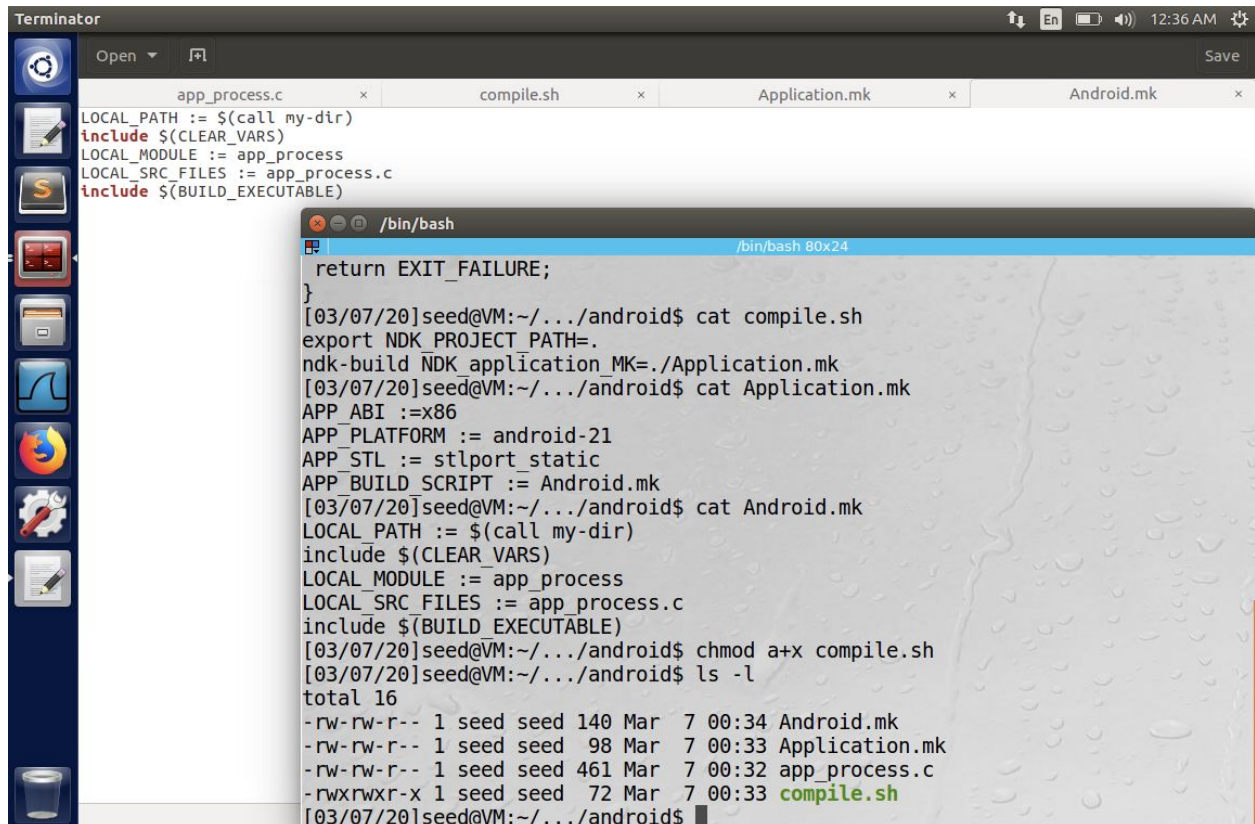
/bin/bash

```
fclose(f);

// Launch the original binary
char * cmd = "/system/bin/app_process_original";
execve(cmd, argv, environ);

// execve () returns only if it fails
return EXIT_FAILURE;
}
```

```
[03/07/20]seed@VM:~/.../android$ cat compile.sh
export NDK_PROJECT_PATH=.
ndk-build NDK_APPLICATION_MK=./Application.mk
[03/07/20]seed@VM:~/.../android$ cat Application.mk
APP_ABI :=x86
APP_PLATFORM := android-21
APP_STL := stlport static
APP_BUILD_SCRIPT := Android.mk
[03/07/20]seed@VM:~/.../android$ cat Android.mk
LOCAL_PATH := $(call my-dir)
include $(CLEAR_VARS)
LOCAL_MODULE := app_process
LOCAL_SRC_FILES := app_process.c
include $(BUILD_EXECUTABLE)
[03/07/20]seed@VM:~/.../android$
```

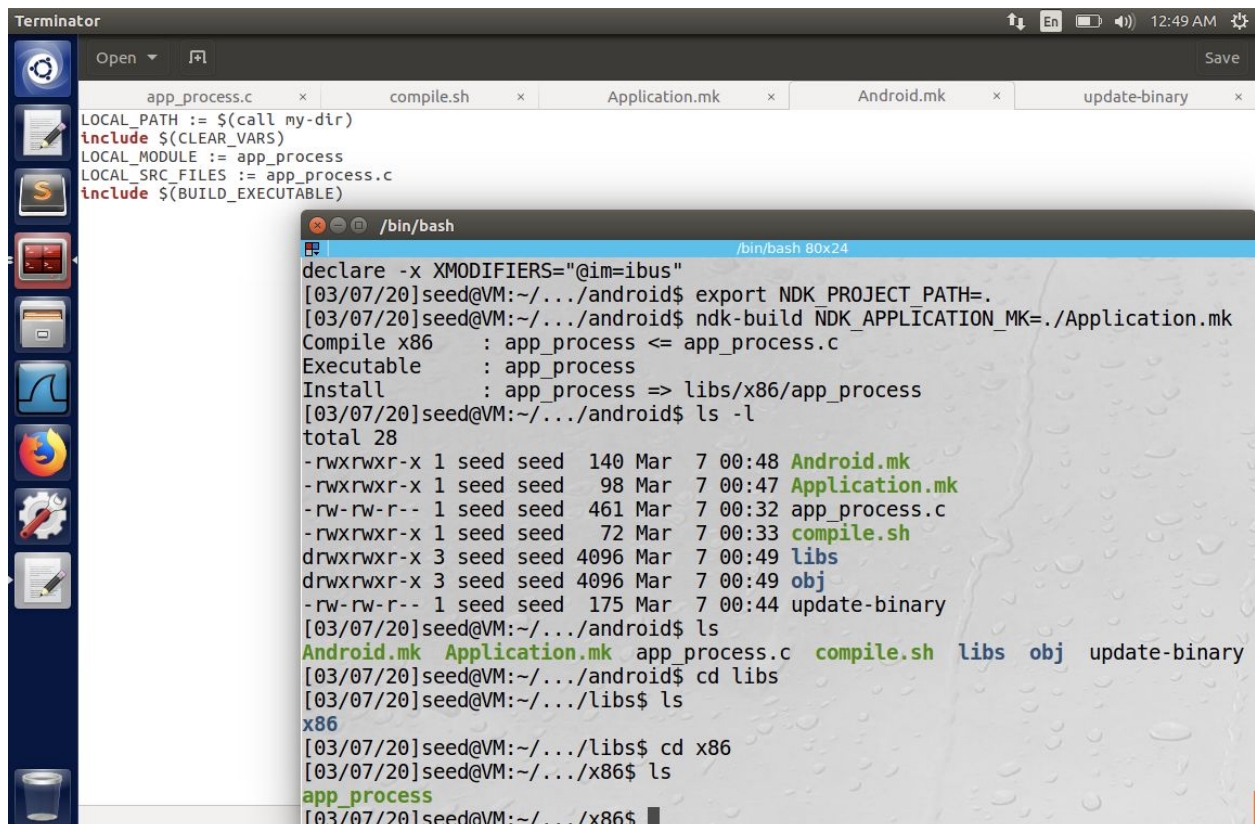
The Terminator window displays four file tabs: `app_process.c`, `compile.sh`, `Application.mk`, and `Android.mk`. The `app_process.c` tab is active, showing the following content:

```
LOCAL_PATH := $(call my-dir)
include $(CLEAR_VARS)
LOCAL_MODULE := app_process
LOCAL_SRC_FILES := app_process.c
include $(BUILD_EXECUTABLE)
```

The terminal window, titled `/bin/bash`, shows the following commands and output:

```
/bin/bash 80x24
return EXIT_FAILURE;
}
[03/07/20]seed@VM:~/.../android$ cat compile.sh
export NDK_PROJECT_PATH=.
ndk-build NDK_APPLICATION_MK=./Application.mk
[03/07/20]seed@VM:~/.../android$ cat Application.mk
APP_ABI :=x86
APP_PLATFORM := android-21
APP_STL := stlport_static
APP_BUILD_SCRIPT := Android.mk
[03/07/20]seed@VM:~/.../android$ cat Android.mk
LOCAL_PATH := $(call my-dir)
include $(CLEAR_VARS)
LOCAL_MODULE := app_process
LOCAL_SRC_FILES := app_process.c
include $(BUILD_EXECUTABLE)
[03/07/20]seed@VM:~/.../android$ chmod a+x compile.sh
[03/07/20]seed@VM:~/.../android$ ls -l
total 16
-rw-rw-r-- 1 seed seed 140 Mar  7 00:34 Android.mk
-rw-rw-r-- 1 seed seed  98 Mar  7 00:33 Application.mk
-rw-rw-r-- 1 seed seed 461 Mar  7 00:32 app_process.c
-rwxrwxr-x 1 seed seed  72 Mar  7 00:33 compile.sh
[03/07/20]seed@VM:~/.../android$
```

Transferring task2.zip to android VM

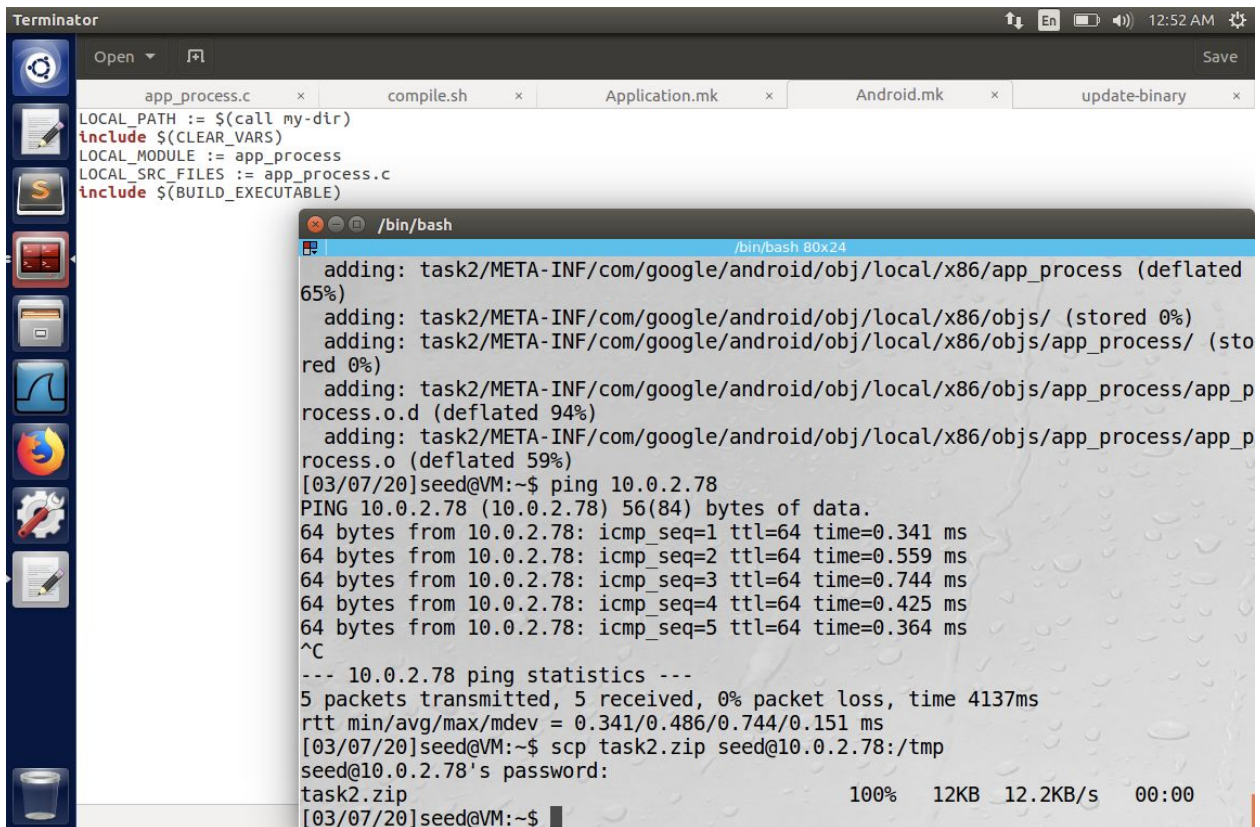


The Terminator window displays five file tabs: `app_process.c`, `compile.sh`, `Application.mk`, `Android.mk`, and `update-binary`. The `app_process.c` tab is active, showing the same content as in the previous screenshot.

The terminal window, titled `/bin/bash`, shows the following commands and output:

```
/bin/bash 80x24
declare -x XMODIFIERS="@im=ibus"
[03/07/20]seed@VM:~/.../android$ export NDK_PROJECT_PATH=.
[03/07/20]seed@VM:~/.../android$ ndk-build NDK_APPLICATION_MK=./Application.mk
Compile x86      : app_process <= app_process.c
Executable      : app_process
Install         : app_process => libs/x86/app_process
[03/07/20]seed@VM:~/.../android$ ls -l
total 28
-rwxrwxr-x 1 seed seed  140 Mar  7 00:48 Android.mk
-rwxrwxr-x 1 seed seed   98 Mar  7 00:47 Application.mk
-rw-rw-r-- 1 seed seed 461 Mar  7 00:32 app_process.c
-rwxrwxr-x 1 seed seed  72 Mar  7 00:33 compile.sh
drwxrwxr-x 3 seed seed 4096 Mar  7 00:49 libs
drwxrwxr-x 3 seed seed 4096 Mar  7 00:49 obj
-rw-rw-r-- 1 seed seed 175 Mar  7 00:44 update-binary
[03/07/20]seed@VM:~/.../android$ ls
Android.mk Application.mk app_process.c compile.sh libs obj update-binary
[03/07/20]seed@VM:~/.../android$ cd libs
[03/07/20]seed@VM:~/.../libs$ ls
x86
[03/07/20]seed@VM:~/.../libs$ cd x86
[03/07/20]seed@VM:~/.../x86$ ls
app_process
[03/07/20]seed@VM:~/.../x86$
```

With this, we have given permission to execute compile.sh
Running compile.sh gives us app_process as well as the obj and libs file, which we will now zip
and move into the android VM

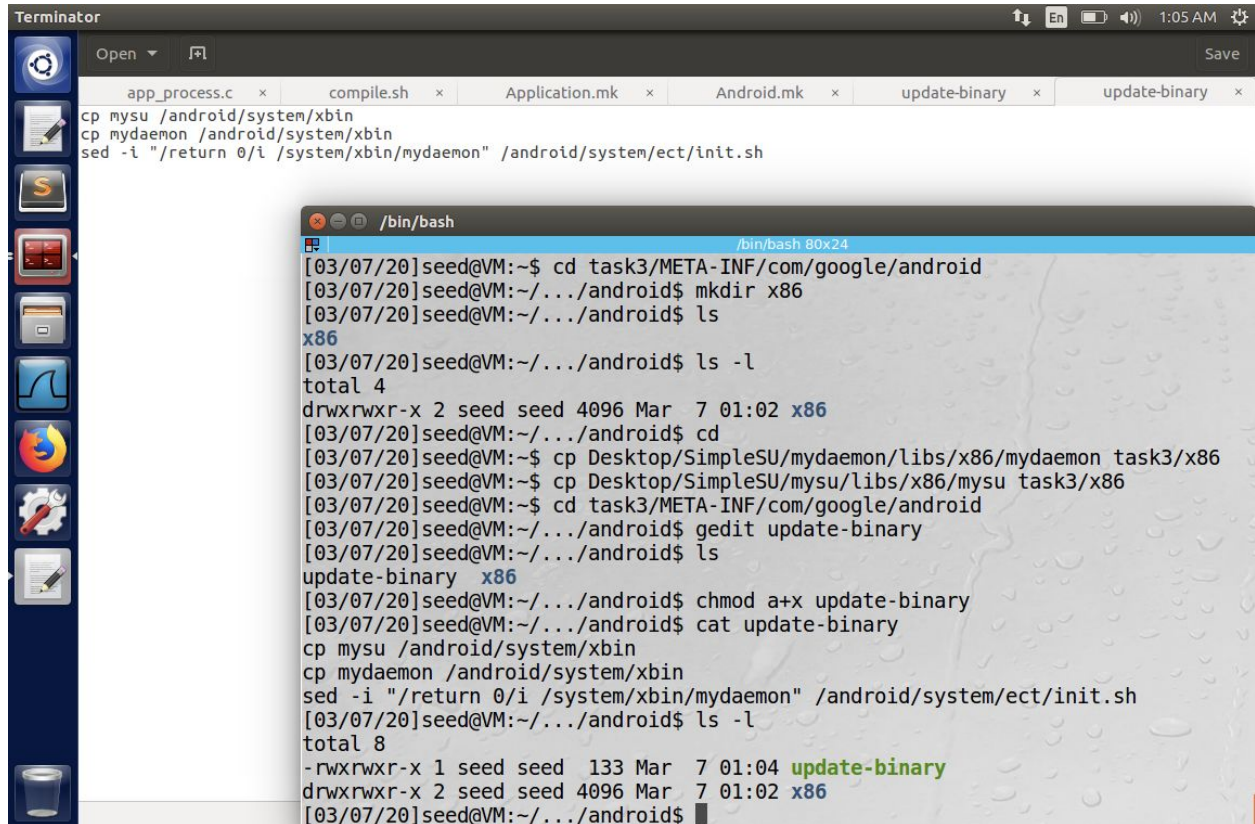


```
Terminator
Open Save
app_process.c x compile.sh x Application.mk x Android.mk x update-binary x
LOCAL_PATH := $(call my-dir)
include $(CLEAR_VARS)
LOCAL_MODULE := _app_process
LOCAL_SRC_FILES := app_process.c
include $(BUILD_EXECUTABLE)

/bin/bash
/bin/bash 80x24
adding: task2/META-INF/com/google/android/obj/local/x86/app_process (deflated
65%)
adding: task2/META-INF/com/google/android/obj/local/x86/objs/ (stored 0%)
adding: task2/META-INF/com/google/android/obj/local/x86/objs/app_process/ (sto
red 0%)
adding: task2/META-INF/com/google/android/obj/local/x86/objs/app_process/app_p
rocess.o.d (deflated 94%)
adding: task2/META-INF/com/google/android/obj/local/x86/objs/app_process/app_p
rocess.o (deflated 59%)
[03/07/20]seed@VM:~$ ping 10.0.2.78
PING 10.0.2.78 (10.0.2.78) 56(84) bytes of data.
64 bytes from 10.0.2.78: icmp_seq=1 ttl=64 time=0.341 ms
64 bytes from 10.0.2.78: icmp_seq=2 ttl=64 time=0.559 ms
64 bytes from 10.0.2.78: icmp_seq=3 ttl=64 time=0.744 ms
64 bytes from 10.0.2.78: icmp_seq=4 ttl=64 time=0.425 ms
64 bytes from 10.0.2.78: icmp_seq=5 ttl=64 time=0.364 ms
^C
--- 10.0.2.78 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4137ms
rtt min/avg/max/mdev = 0.341/0.486/0.744/0.151 ms
[03/07/20]seed@VM:~$ scp task2.zip seed@10.0.2.78:/tmp
seed@10.0.2.78's password:
task2.zip
100% 12KB 12.2KB/s 00:00
[03/07/20]seed@VM:~$
```

Task 2 has successfully been transferred to the android VM

Following running bash compile_all from the SudoSU.zip file provided, we create the following
update-binary script and zip it to the task3 file

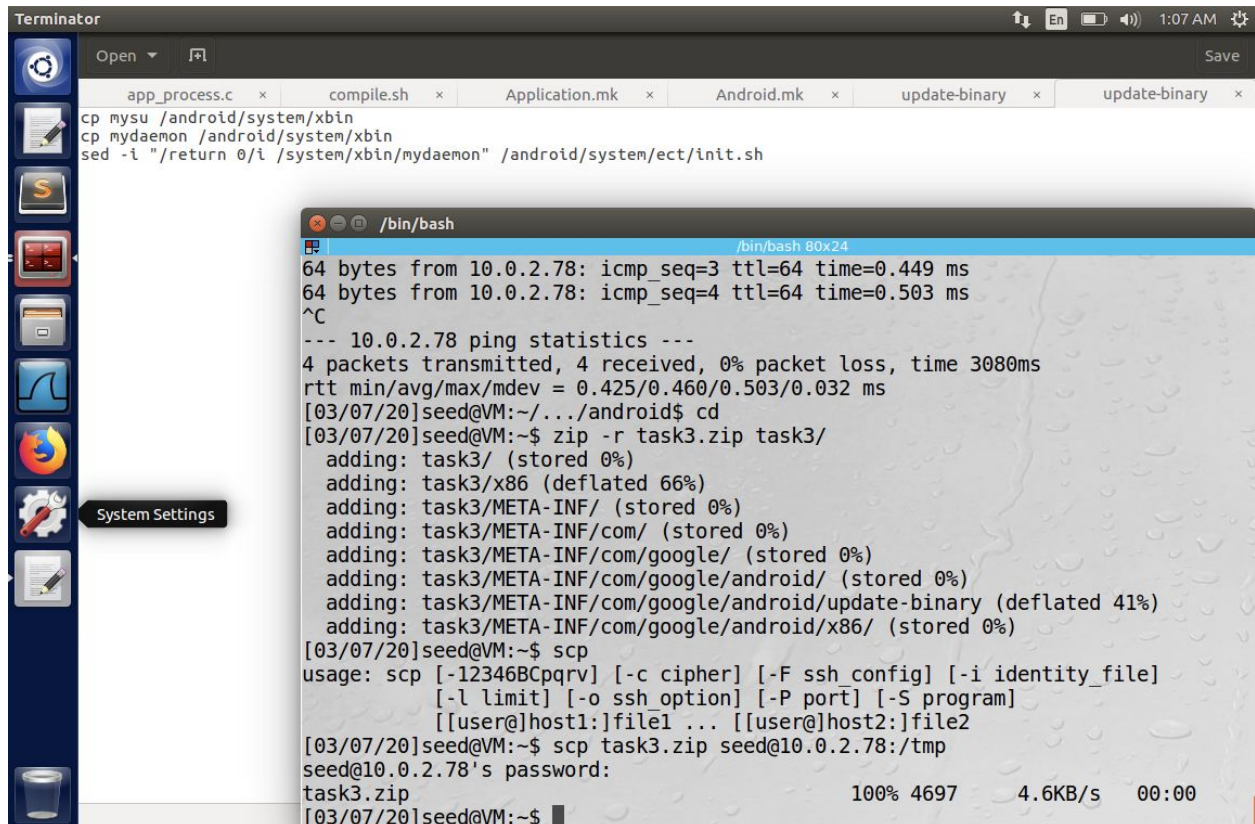


The image shows a Terminator window with a top bar containing icons for Open, Save, and a status bar with 'En', battery, and time '1:05 AM'. The main pane has a tabbed interface with files: app_process.c, compile.sh, Application.mk, Android.mk, update-binary, and update-binary. The terminal content shows the following commands and output:

```
cp mysu /android/system/xbin
cp mydaemon /android/system/xbin
sed -i "/return 0/i /system/xbin/mydaemon" /android/system/etc/init.sh

/bin/bash
[03/07/20]seed@VM:~$ cd task3/META-INF/com/google/android
[03/07/20]seed@VM:~/.../android$ mkdir x86
[03/07/20]seed@VM:~/.../android$ ls
x86
[03/07/20]seed@VM:~/.../android$ ls -l
total 4
drwxrwxr-x 2 seed seed 4096 Mar  7 01:02 x86
[03/07/20]seed@VM:~/.../android$ cd
[03/07/20]seed@VM:~$ cp Desktop/SimpleSU/mydaemon/libs/x86/mydaemon task3/x86
[03/07/20]seed@VM:~$ cp Desktop/SimpleSU/mysu/libs/x86/mysu task3/x86
[03/07/20]seed@VM:~$ cd task3/META-INF/com/google/android
[03/07/20]seed@VM:~/.../android$ gedit update-binary
[03/07/20]seed@VM:~/.../android$ ls
update-binary x86
[03/07/20]seed@VM:~/.../android$ chmod a+x update-binary
[03/07/20]seed@VM:~/.../android$ cat update-binary
cp mysu /android/system/xbin
cp mydaemon /android/system/xbin
sed -i "/return 0/i /system/xbin/mydaemon" /android/system/etc/init.sh
[03/07/20]seed@VM:~/.../android$ ls -l
total 8
-rwxrwxr-x 1 seed seed 133 Mar  7 01:04 update-binary
drwxrwxr-x 2 seed seed 4096 Mar  7 01:02 x86
[03/07/20]seed@VM:~/.../android$
```

We send it to the Android VM...



The image shows a Terminator window with the same top bar as the previous one, but the time is '1:07 AM'. The main pane has the same tabbed interface. The terminal content shows the following commands and output:

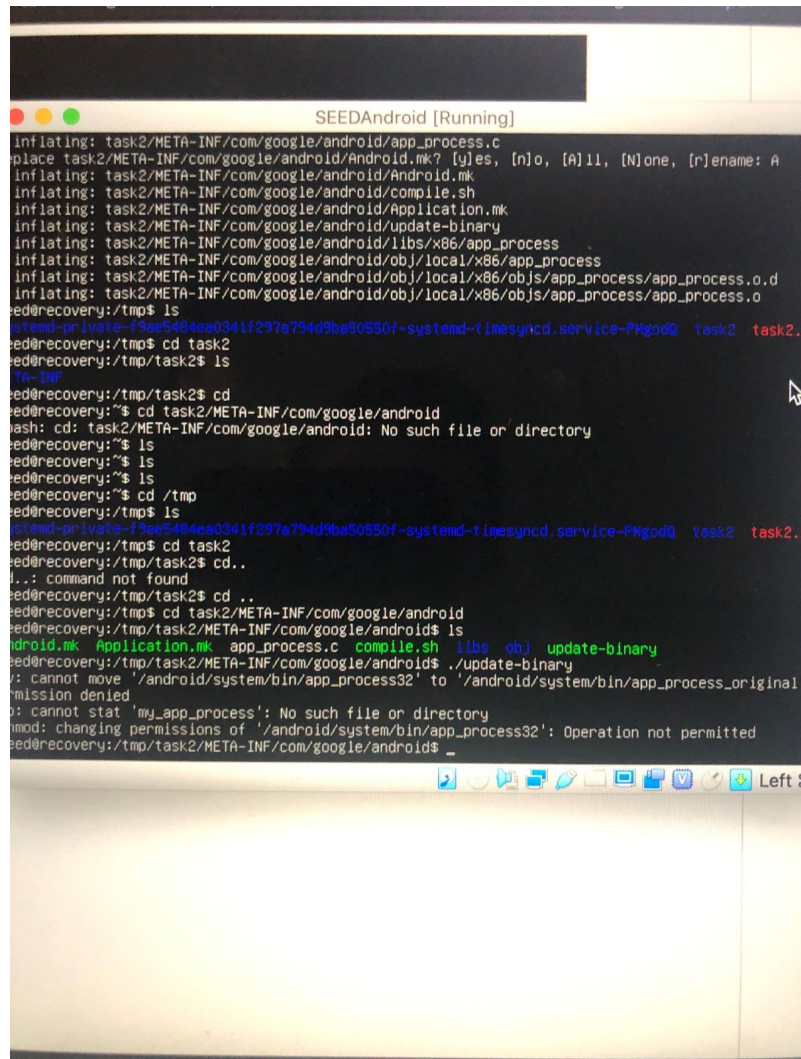
```
cp mysu /android/system/xbin
cp mydaemon /android/system/xbin
sed -i "/return 0/i /system/xbin/mydaemon" /android/system/etc/init.sh

/bin/bash
64 bytes from 10.0.2.78: icmp_seq=3 ttl=64 time=0.449 ms
64 bytes from 10.0.2.78: icmp_seq=4 ttl=64 time=0.503 ms
^C
--- 10.0.2.78 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.425/0.460/0.503/0.032 ms
[03/07/20]seed@VM:~/.../android$ cd
[03/07/20]seed@VM:~$ zip -r task3.zip task3/
adding: task3/ (stored 0%)
adding: task3/x86 (deflated 66%)
adding: task3/META-INF/ (stored 0%)
adding: task3/META-INF/com/ (stored 0%)
adding: task3/META-INF/com/google/ (stored 0%)
adding: task3/META-INF/com/google/android/ (stored 0%)
adding: task3/META-INF/com/google/android/update-binary (deflated 41%)
adding: task3/META-INF/com/google/android/x86/ (stored 0%)
[03/07/20]seed@VM:~$ scp
usage: scp [-12346BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file]
          [-l limit] [-o ssh_option] [-P port] [-S program]
          [[user@]host1:]file1 ... [[user@]host2:]file2
[03/07/20]seed@VM:~$ scp task3.zip seed@10.0.2.78:/tmp
seed@10.0.2.78's password:
task3.zip
100% 4697 4.6KB/s 00:00
[03/07/20]seed@VM:~$
```

A 'System Settings' button is visible on the left sidebar of the Terminator window.

Following sending task3.zip to the android VM, we use the recovery OS in order to launch the code we have sent and get root access #who am i

Sorry if the screenshots of android VM are low, it would not let me screenshot via my computer...



```
SEEDAndroid [Running]
inflating: task2/META-INF/com/google/android/app_process.c
place task2/META-INF/com/google/android/Android.mk? [y]es, [n]o, [A]ll, [N]one, [r]ename: A
inflating: task2/META-INF/com/google/android/Android.mk
inflating: task2/META-INF/com/google/android/compile.sh
inflating: task2/META-INF/com/google/android/Application.mk
inflating: task2/META-INF/com/google/android/update-binary
inflating: task2/META-INF/com/google/android/libs/x86/app_process
inflating: task2/META-INF/com/google/android/obj/local/x86/app_process
inflating: task2/META-INF/com/google/android/obj/local/x86/obj/app_process/app_process.o.d
inflating: task2/META-INF/com/google/android/obj/local/x86/obj/app_process/app_process.o
red@recovery:/tmp$ ls
system-private-t9ae5484ea0341f297a794d9ba50550f-systemd-timesyncd.service-PHgodQ task2 task2..
red@recovery:/tmp$ cd task2
red@recovery:/tmp/task2$ ls
META-INF
red@recovery:/tmp/task2$ cd
red@recovery:/tmp$ cd task2/META-INF/com/google/android
bash: cd: task2/META-INF/com/google/android: No such file or directory
red@recovery:/tmp$ ls
red@recovery:/tmp$ ls
red@recovery:/tmp$ ls
red@recovery:/tmp$ cd /tmp
red@recovery:/tmp$ ls
system-private-t9ae5484ea0341f297a794d9ba50550f-systemd-timesyncd.service-PHgodQ task2 task2..
red@recovery:/tmp$ cd task2
red@recovery:/tmp/task2$ cd..
bash: cd: command not found
red@recovery:/tmp/task2$ cd ..
red@recovery:/tmp$ cd task2/META-INF/com/google/android
red@recovery:/tmp/task2/META-INF/com/google/android$ ls
Android.mk Application.mk app_process.c compile.sh libs obj update-binary
red@recovery:/tmp/task2/META-INF/com/google/android$ ./update-binary
./: cannot move '/android/system/bin/app_process32' to '/android/system/bin/app_process_original'
permission denied
./: cannot stat 'my_app_process': No such file or directory
chmod: changing permissions of '/android/system/bin/app_process32': Operation not permitted
red@recovery:/tmp/task2/META-INF/com/google/android$ _
```