

TERMINAL CHALLENGE

Terminal Recap

TERMINAL VS TERMINAL EMULATOR



TERMINAL:

- RESEMBLES A TYPEWRITER, DOESN'T IT?
- “.. IS AN ELECTRONIC OR ELECTROMECHANICAL HARDWARE DEVICE THAT IS USED FOR ENTERING DATA INTO, AND DISPLAYING DATA FROM, A COMPUTER OR A COMPUTING SYSTEM” - WIKI
- *ENTER DATA*
- *DISPLAY DATA*

TERMINAL VS TERMINAL EMULATOR (CONTINUED)

```
asselaliyeva — -bash — 132x28
Last login: Mon Jul 31 22:29:55 on ttys004
Vanquish:~ russian_mobster$ which $SHELL
/bin/bash
Vanquish:~ russian_mobster$ [obj] = get_instruction(cm, op_value, insns[idx:], self.odex)
6482
6483      # emit instruction

/srv/vasilek/androguard/androguard/core/bytecodes/dvm.py in get_instruction(cm, op_
6390      return InstructionInvalid(cm, buff)
6391      try:
-> 6392      return DALVIK_OPCODES_FORMAT[op_value][0](cm, buff)
6393      except KeyError:
6394      return InstructionInvalid(cm, buff)

KeyboardInterrupt:

In [68]: for current_class in d.get_classes():
...:     for method in current_class.get_methods():
...:         byte_code = method.get_code()
...:         print(byte_code)
...:         if byte_code != None:
...:             bytec = byte_code.get_bc()
...:             idx = 0
...:             for i in bytec.get_instructions():
...:                 if i !=None:
...:                     print(i.get_operands())
...: 
```

TERMINAL EMULATOR:

- EMULATOR
- IMITATES TEXT TERMINAL
- RUNS A SHELL PROGRAM

TERMINAL EMULATOR VS SHELL

TERMINAL EMULATOR:

- AN EMULATOR
- IMITATES TEXT TERMINAL
- RUNS A SHELL PROGRAM

SHELL:

- A PROGRAM
- PARSES THE INPUTS
- STARTS OTHER PROGRAMS
- BASH, SH, FISH, ETC.

TERMINAL COMMANDS

`ls` - lists all of the files in the directory

`cd folder_name` - change to the specified directory

`cat file_name` - show the contents of the file

`vim` - text editor

`man command` - your best friend! Gives you a full description of the command

Many many more cool commands ...

You may find [this](#) helpful! Or Google ;)

CHALLENGE SETUP

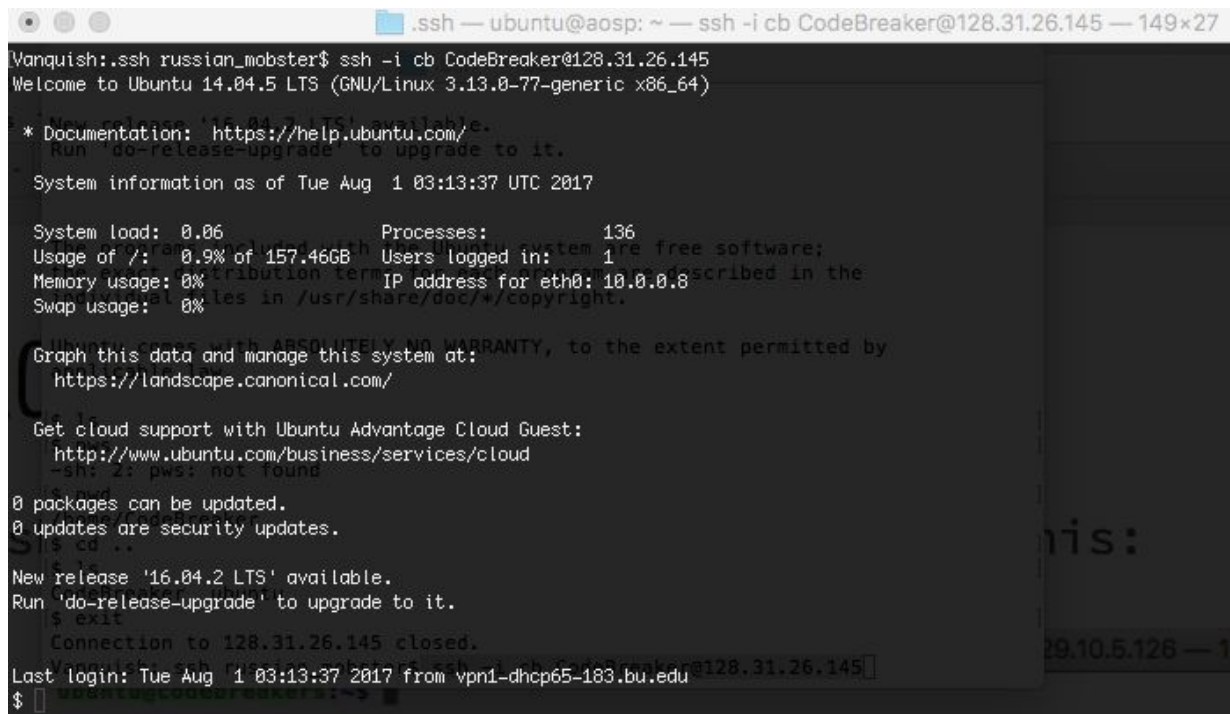
- DOWNLOAD A FILE CALLED “CB” FROM GITHUB
- RUN `chmod 700 CH`
- `SSH -I CB CODEBREAKER@128.31.26.145`

CHALLENGE SETUP (CONTINUED)

You should end up with something like this ->

Congratulations!

You have control over a remote machine!



```
.ssh — ubuntu@aosp: ~ — ssh -i cb CodeBreaker@128.31.26.145 — 149x27
Vanquish:ssh russian_mobster$ ssh -i cb CodeBreaker@128.31.26.145
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
   Run 'do-release-upgrade' to upgrade to it.

System information as of Tue Aug  1 03:13:37 UTC 2017

System load: 0.06               Processes:           136
Usage of /:  0.9% of 157.46GB    Users logged in:     1
Memory usage: 0%                IP address for eth0: 10.0.0.8
Swap usage:  0%

Graph this data and manage this system at:
https://landscape.canonical.com/

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

New release '16.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
$ exit
Connection to 128.31.26.145 closed.
Last login: Tue Aug  1 03:13:37 2017 from vpn1-dhcp65-183.bu.edu
$
```

TERMINAL CHALLENGE

- What is the path of the directory you are currently in?
- What is your username on the remote machine?
- Implement the instruction described in the file *cbReadMe* under *bin* directory
- List all the files in */var/tmp*. Who is the owner of the *BU* file?
- “He held out his snuffbox of old gold, with a great amethyst in the centre of the lid.”. Does *merlinorearlyhis04wheauoft.txt* contain this string?
- Go back to your original directory
- Make a folder named “your name here”
- Change to that directory. Create and edit *my_message.txt* with any text editor (you can use *vim* or *nano*)
- Find somebody else’s message and read it!
- Copy any file from your local machine (!) to the directory you made on the remote *CodeBreaker@128.31.26.145* [Hint](#)

TERMINAL CHALLENGE (CONTINUED)

- What Python version does the server use?
- What is the Python source directory?
- What is the speed of CPU of the server?
- What file is located under `tmp` directory? What message does it print?
- Find public key corresponding to your private key hidden somewhere on the server (Think of where RSA keys are saved on Linux)
- What code is hidden in `lizard.jpg.uue` in your home directory?
- If the second server has `ip==10.0.0.61`, is it reachable from a public network? (Internet)
- What is the code in `topsecret.txt` in ubuntu's home directory?