

Cyberpaths

- CTF Password Lab -

by Marco Lin

PART 1, SETTING UP THE TECHNOLOGY

The screenshot shows the Cyberpath interface. On the left, there's a sidebar titled "Drag to Add" with icons for VM, Xen VM, EG VM, Raw PC IG, Raw PC EQ, and OF OVS. Below it is a "New Site" button. The main area displays a network diagram with nodes labeled pivot, alice, bob, carol, and david. Node pivot is connected to node alice. Node alice is connected to nodes bob and carol. Node bob is connected to node carol. Node carol is connected to node david. A label "Site 1" is positioned near node alice. At the top right of the interface are buttons for "Delete All", "New View", and "View RSpec". Below the diagram, the version "v1.6" is visible.

Below the diagram is an RSpec editor interface. It has tabs for "Portal", "File", "URL", and "Text Box". The "Text Box" tab is active, showing XML code for the RSpec. The XML includes namespaces for geni, emulab, protogeni, and ext(jacks). The "Choose RSpec" section is orange and contains a "Save RSpec" button and "Editor Ops" buttons for "Expand", "Duplicate Nodes only", "Auto IP", and "Add Global Node". The status bar at the bottom says "This RSpec is valid."

Run the following commands on each machine:

sudo python /local/setup.py

The terminal window shows the execution of the setup.py script on multiple hosts. The session starts with a connection from marco@carol to m_lin23@carol. It then shows attempts to run setup.py on m_lin23@carol, which fails because sudo is not found. Subsequent attempts to run setup.py on m_lin23@carol also fail. Finally, a successful run of setup.py is shown on m_lin23@carol, resulting in the message "carol".

```
marco@marco-m-OptiPlex-5070:~$ ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29212 -t 96x28
...2 - ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 26210 ...ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29212 +
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[pc2.instageni.colorado.edu]:29212,[192.12.245.142]:29212' (RSA) to the list of known hosts.
[Enter passphrase for key '/Users/marco/.ssh/id_geni_ssh_rsa']:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-154-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

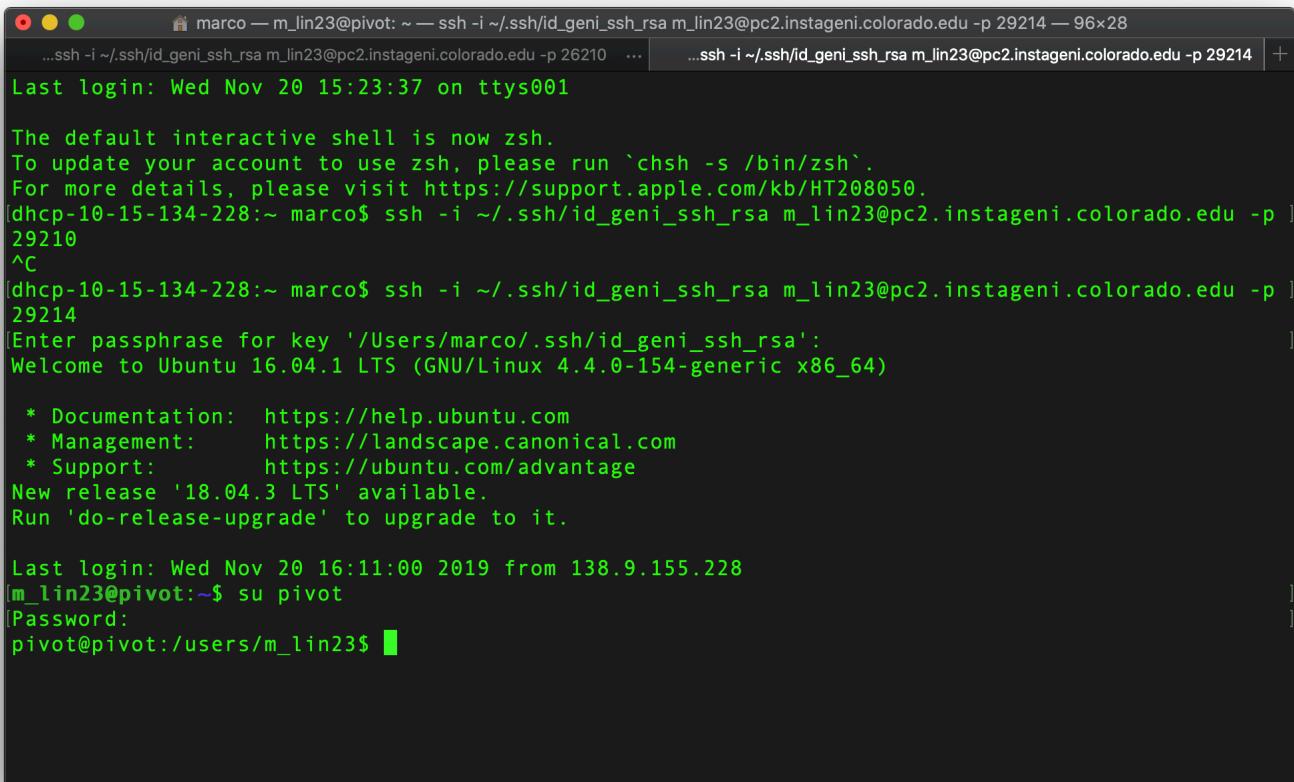
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

m_lin23@carol:~$ sudo python /local/setup.py
sudo: python: command not found
m_lin23@carol:~$ sudo python /local/setup.py
sudo: python: command not found
m_lin23@carol:~$ sudo python /local/setup.py
sudo: python: command not found
m_lin23@carol:~$ sudo python /local/
local/      lost+found/
m_lin23@carol:~$ sudo python /local/setup.py
carol
m_lin23@carol:~$
```

PART 2, THE MISSION

1. Using a pivot machine



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there are three small circular icons (red, yellow, green). Below them, the title bar displays the user 'marco' and the host 'm_lin23@pivot'. The main area of the terminal shows a series of SSH commands being run:

```
marco — m_lin23@pivot: ~ — ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29214 — 96x28
...ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 26210 ...
...ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29214 +
```

Following these commands, the terminal displays a standard Ubuntu 16.04 LTS login screen with a welcome message and upgrade information. Finally, it shows a root shell prompt:

```
Last login: Wed Nov 20 15:23:37 on ttys001
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
[dhcp-10-15-134-228:~ marco$ ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29210
^C
[dhcp-10-15-134-228:~ marco$ ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29214
[Enter passphrase for key '/Users/marco/.ssh/id_geni_ssh_rsa']:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-154-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Nov 20 16:11:00 2019 from 138.9.155.228
[m_lin23@pivot:~$ su pivot
[Password:
pivot@pivot:/users/m_lin23$ ]
```

2. Find the password and login to Alice's machine

```
marco — m_lin23@pivot: ~ — ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29214 — 96x28
...ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 26210 ... ...ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29214 +
[pivot@pivot:~/Desktop$ cat password.txt
Alice's password: password
Alice's password: password
[pivot@pivot:~/Desktop$ ssh alice@alice
The authenticity of host 'alice (10.10.1.2)' can't be established.
RSA key fingerprint is SHA256:FVGYdB+vTgZ99/f8auDcyKwJU8h0pw3xaAmj4MQF54Q.
[Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'alice,10.10.1.2' (RSA) to the list of known hosts.
[alice@alice's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-154-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage
New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

[$ whoami
alice
$
```

3. Find the bob's password

```
[~] $ ls
Desktop Documents Downloads Music Pictures Videos
[~] $ cd Document
[~] -sh: 5: cd: can't cd to Document
[~] $ cd Documents
[~] $ ls
mySecret
[~] $ cat mySecret
cat: mySecret: Is a directory
[~] $ cd mySecret
[~] $ ls
password.txt
[~] $ cat password.txt
Yggv bgt xafvafy lzak hskkogjy sfv xaymjafy gml ozsl wfujqhlaf al mkwv... lzw fwpl gfw ogf'l tw
kg wskq, lzgmyz.
Tgt'k Hskkogjv: hdsلافme
[~] $ vim password.txt
[~] $ cat password.txt
Yggv bgt xafvafy lzak hskkogjv sfv xaymjafy gml ozsl wfujqhlaf al mkwv... lzw fwpl gfw ogf'l tw
kg wskq, lzgmyz.
Tgt'k Hskkogjv: hdsلافme
[~] $
```

4. Crack bob's password by using the Ciphers and codes website.

Cryptogram Solver

Rumkin.com >> Web-Based Tools >> Ciphers and Codes

Search:

Do you have a cryptogram, also known as a cryptoquip or a simple letter substitution cipher? Just type it in here and get it solved within seconds. If there are lots of possible solutions, only a subset will be shown. This page does send your cryptogram to my server, so you might not want to use it if your message is extremely sensitive and you think that I care about what you are submitting. Also, only words that are found in my dictionary will be found. If there are proper names or misspellings, it may cause the puzzle to be unsolved.

Warning: Offensive results can be generated. This simply uses all of the words in several dictionaries. The dictionaries list words of varying offensiveness because, well, they are still words. Use of this tool implies that you understand that the risks of what you may see.

Dictionary: American English (Medium)

```
Ygvg bgt xavafy izak hskkogiv sfv xaymjafy gml ozsl  
wfujhlagf al mkwv... lzw fwpl gfw ogf! tw kg wska,  
lzgmyz  
Tgt'k Hskkogiv: hdslafme
```

The Results

GOOD JOB FINDING THIS PASSWORD AND FIGURING OUT WHAT ENCRYPTION IT USED THE NEXT ONE WON'T BE SO EASY THOUGH BOB'S PASSWORD PLATINUM

5. Login bob's machine

```
marco — m_lin23@pivot: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29214 — 80x24
[alice@alice's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-154-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Nov 20 23:16:24 2019 from 10.10.1.1
[$ ssh bob@bob
[bob@bob's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-154-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Nov 20 23:30:39 2019 from 10.10.2.1
[$ whoami
bob
$ ]
```

6. Find the carol's password which is hidden file under Music folder.

```

marco — m_lin23@pivot: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29214 — 80x24

Last login: Wed Nov 20 23:16:24 2019 from 10.10.1.1
[$ ssh bob@bob
[bob@bob's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-154-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage
New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Nov 20 23:30:39 2019 from 10.10.2.1
[$ whoami
[bob
[$ ls
Desktop Documents Downloads Music Pictures Videos
[$ cd Music
[$ ls
all_journey_songs.wav best_of_classical_music.wav smooth_jaz.mp3
[$ ls -a
. .password.txt best_of_classical_music.wav
.. all_journey_songs.wav smooth_jaz.mp3
$ █

```

7. Get the password

```

~ — m_lin23@client: ~ — -bash ... ~ — m_lin23@pivot: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29214 +
Nice job finding the hidden file - here is Carol's password, but it is encrypted...
Carol's Password: 8601f6e1028a8e8a966f6c33fcd9aec4
~ ~

```

8. Crack the password by using the website Crack Station.

The screenshot shows the CrackStation website interface. At the top, there is a navigation bar with links for 'CrackStation', 'Password Hashing Security', 'Defuse Security', 'Defuse.ca', and 'Twitter'. Below the navigation bar, the main title 'CrackStation' is displayed in large, bold letters. Underneath the title, there is a sub-header 'Free Password Hash Cracker'. A text input field is present with the placeholder 'Enter up to 20 non-salted hashes, one per line:' followed by the password hash '8601f6e1028a8e8a966f6c33fcd9aec4'. To the right of the input field is a reCAPTCHA verification box with the text '我不是機器人' and a checkbox labeled 'I'm not a robot'. Below the reCAPTCHA is a button labeled 'Crack Hashes'. At the bottom of the page, there is a table with the following data:

Hash	Type	Result
8601f6e1028a8e8a966f6c33fcd9aec4	md5	maxwell

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

9. Login to carol's machine

```
[marco — m_lin23@pivot: ~ — ssh -i ~/ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29214 — 80x24]$ whoami
bob
[$ ls
Desktop Documents Downloads Music Pictures Videos
[$ cd Music
[$ ls
all_journey_songs.wav best_of_classical_music.wav smooth_jaz.mp3
[$ ls -a
. .password.txt best_of_classical_music.wav
.. all_journey_songs.wav smooth_jaz.mp3
[$ ssh carol@carol
[carol@carol's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-154-generic x86_64)

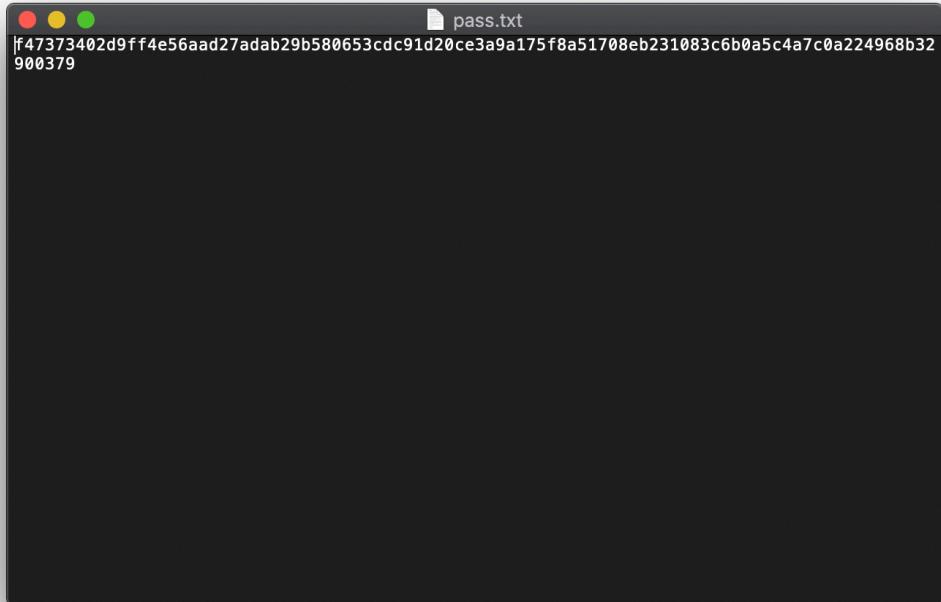
 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage
New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Nov 21 00:04:30 2019 from 10.10.3.1
[$ whoami
carol
$
```

10. Looking for David's password which is under documents folder and the name of the file is password3.txt

```
[\$ cd ..
[\$ ls
Desktop Documents Downloads Music Pictures Videos
[\$ cd Documents
[\$ ls
password0.txt password1.txt password2.txt password3.txt password4.txt password5.txt
[\$ cat password0.txt
[\$ cat password1.txt
[\$ cat password2.txt
[\$ cat password3.txt
You found the final password, but it is encrypted again!
David's Password: f47373402d9ff4e56aad27adab29b580653cdc91d20ce3a9a175f8a51708eb231083c6b0a5c4a7
c0a224968b32900379
\$
```

We can use the tool called john the ripper, we save the password in a text file like the following:



Run the john to crack the file and wait for around 30 min

```
crackPD — john pass.txt — 100x26
0g 0:00:00:12 3/3 0g/s 1767Kp/s 1767KC/s 1767KC/s 3i2..seamoman1
0g 0:00:00:13 3/3 0g/s 1878Kp/s 1878KC/s 1878KC/s cebbi39..cebsin2
0g 0:00:00:14 3/3 0g/s 1949Kp/s 1949KC/s 1949KC/s h1nn..sexicerse
0g 0:00:00:15 3/3 0g/s 2040Kp/s 2040KC/s 2040KC/s tkbtms..tk4n20
0g 0:00:00:16 3/3 0g/s 2116Kp/s 2116KC/s 2116KC/s yu6..1mok00
0g 0:00:00:17 3/3 0g/s 2196Kp/s 2196KC/s 2196KC/s shoempri..shoe1124
0g 0:00:00:18 3/3 0g/s 2266Kp/s 2266KC/s 2266KC/s puy175..puyz05
0g 0:00:00:19 3/3 0g/s 2320Kp/s 2320KC/s 2320KC/s bhscoma..bhscruz
0g 0:00:00:20 3/3 0g/s 2385Kp/s 2385KC/s 2385KC/s 0bt04..sexymoots
0g 0:00:00:21 3/3 0g/s 2439Kp/s 2439KC/s 2439KC/s ary279..aruh13
0g 0:00:00:22 3/3 0g/s 2482Kp/s 2482KC/s 2482KC/s gupp6U..gupeea
0g 0:00:00:23 3/3 0g/s 2528Kp/s 2528KC/s 2528KC/s beekoolf..beek1025
0g 0:00:00:24 3/3 0g/s 2581Kp/s 2581KC/s 2581KC/s nmom01..nmeclh
0g 0:00:00:25 3/3 0g/s 2624Kp/s 2624KC/s 2624KC/s 0n0sin..0n8m80
0g 0:00:00:26 3/3 0g/s 2661Kp/s 2661KC/s 2661KC/s 5hnbf..sexycon01
0g 0:00:00:27 3/3 0g/s 2694Kp/s 2694KC/s 2694KC/s 1857m..170r5
0g 0:00:00:28 3/3 0g/s 2734Kp/s 2734KC/s 2734KC/s alaitito..alysspurl
0g 0:00:00:29 3/3 0g/s 2772Kp/s 2772KC/s 2772KC/s gA3..lovermy7
0g 0:00:00:30 3/3 0g/s 2804Kp/s 2804KC/s 2804KC/s gcth3w..123wf
0g 0:00:00:31 3/3 0g/s 2832Kp/s 2832KC/s 2832KC/s fmboiti..fmblem
0g 0:00:00:32 3/3 0g/s 2866Kp/s 2866KC/s 2866KC/s prayss15..pram1792
0g 0:00:00:33 3/3 0g/s 2895Kp/s 2895KC/s 2895KC/s sb0unt..sb0r16
0g 0:00:00:34 3/3 0g/s 2927Kp/s 2927KC/s 2927KC/s rip1019..rip1452
0g 0:00:00:35 3/3 0g/s 2953Kp/s 2953KC/s 2953KC/s 113oko..11b8up
0g 0:00:00:36 3/3 0g/s 2981Kp/s 2981KC/s 2981KC/s redhds3..redawn4
```

Then we found the password is 55LqdcJM2b6Kw, and we can log into David's machine

```
marco — m_lin23@pivot: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa m_lin23@pc2.insta...
[david@david's password: ]  
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-154-generic x86_64)  
  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
New release '18.04.3 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
[$ whoami ]  
david  
[$ ls ]  
congratulations.txt  
[$ cat congratulations.txt ]  
If you got here, CONGRATS! That's the end!  
$
```