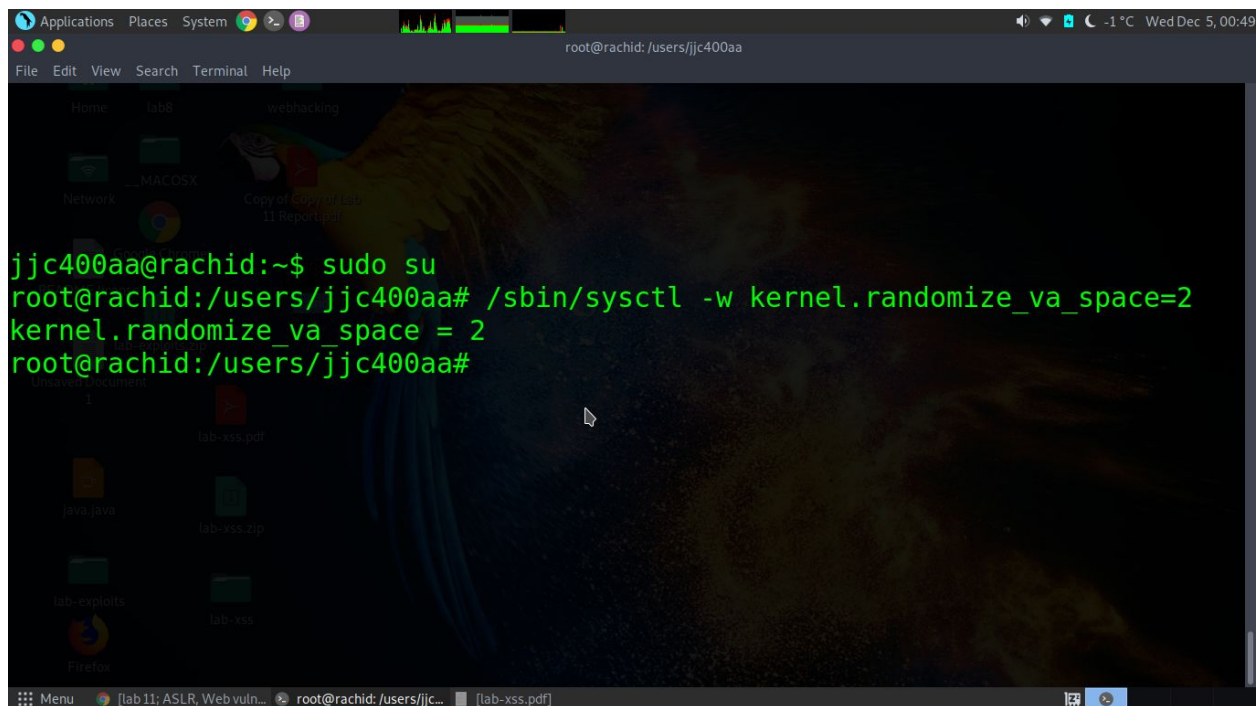


# CSCI 400 Security Lab

## Topic: ASLR, Web vulnerabilities and Encrypted Mail

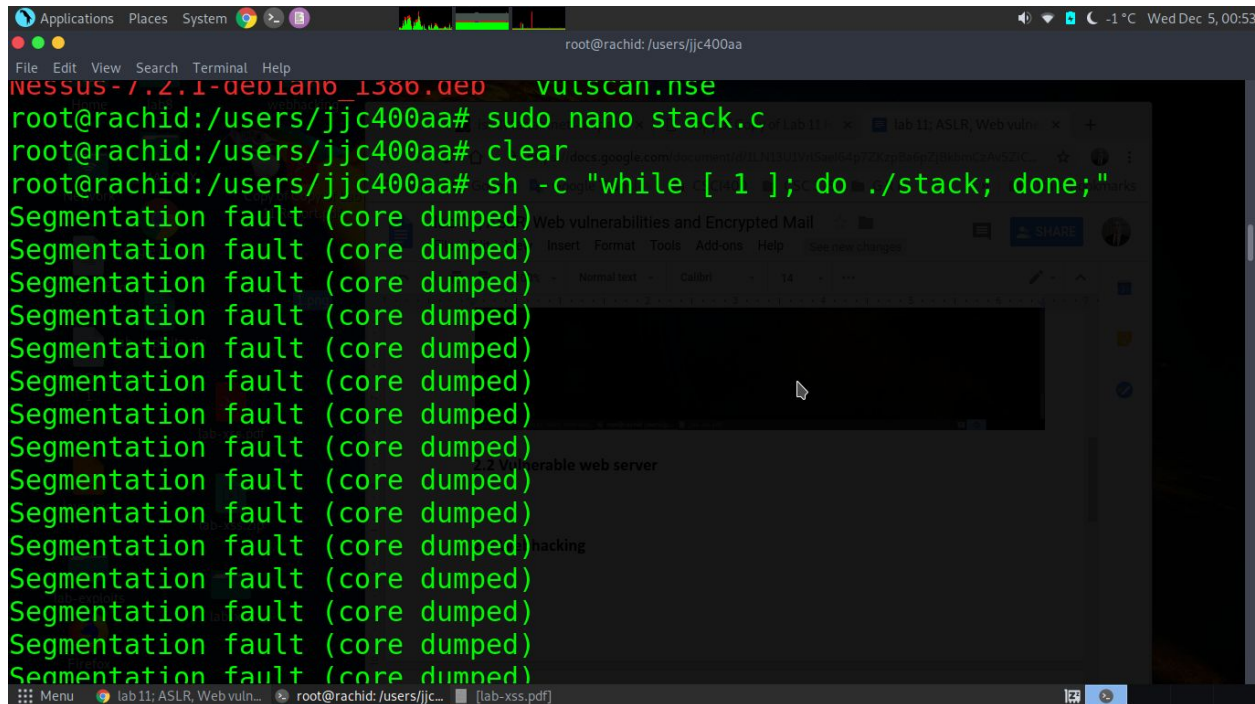
Lab Break Down	
Jennifer Garcia	2.4 Mail security Word Problem 4
Michael Gonzalez	2.3, Word Problems: 1 , 2, 3
Rachid Afaf	2.1 & 2.2
Yevgeniya Martynyuk	

### 2.1 Overcoming ASLR



The screenshot shows a Linux desktop environment with a terminal window open. The terminal prompt is `jjc400aa@rachid:~$`. The user enters `sudo su` to become root. The root prompt is `root@rachid:/users/jjc400aa#`. The user enters `/sbin/sysctl -w kernel.randomize_va_space=2`. The terminal output shows `kernel.randomize_va_space = 2`. The root prompt is `root@rachid:/users/jjc400aa#`. The desktop background is a dark, abstract image. The terminal window has a menu bar with `File Edit View Search Terminal Help`. The desktop has icons for `Home`, `lab8`, `webhacking`, `MACOSX`, `Network`, `Copy of Copy of Lab 11 Report.pdf`, `lab-xss.pdf`, `lab-xss.zip`, `lab-xss`, `lab-exploits`, `java.java`, `Firefox`, and `Firefox`. The system tray at the bottom shows `Menu`, `[lab 11: ASLR, Web vuln...`, `root@rachid: /users/jjc...`, and `[lab-xss.pdf]`. The system status bar at the top right shows `-1°C` and `Wed Dec 5, 00:49`.

```
jjc400aa@rachid:~$ sudo su
root@rachid:/users/jjc400aa# /sbin/sysctl -w kernel.randomize_va_space=2
kernel.randomize_va_space = 2
root@rachid:/users/jjc400aa#
```



```
root@rachid:/users/jjc400aa# sudo nano stack.c
root@rachid:/users/jjc400aa# clear
root@rachid:/users/jjc400aa# sh -c "while [ 1 ]; do ./stack; done;"
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
Segmentation fault (core dumped)
```

**I was not able to invoke the shell !**

## 2.2 Vulnerable web server

I installed apache2 and php5 after that I have set permissions for the extremesecure by the using the following commands:

```
sudo apt - get install apache2 php5
```

```
sudo ln - sv / path / to / extremeinsecure / var / www / html
```

```
chmod 604 extremeinsecure
```

```
chmod 705 extremeinsecure
```

```
chmod + x process . php extremeinsecure
```

```
chmod +x extremeinsecure/_vti_cnf/process.php
```

```
ls -ltr extremeinsecure/process.php
```

```
/etc/apache2/mods-enabled/dir.conf to prioritize PHP
```

```
/etc/init.d/apache2 start
```

<http://localhost/XSS/setgetcookie.htm>

<http://localhost/XSS/malURL.htm>

They were many .htm files and .php are not properly functioning because each time I tried to excute them, I get an error stating that I shoudl make new line when. Even I added the proper syntax like <!DOCTYPE html> and fixing other error, it keeps pointing to the first line in the process.php

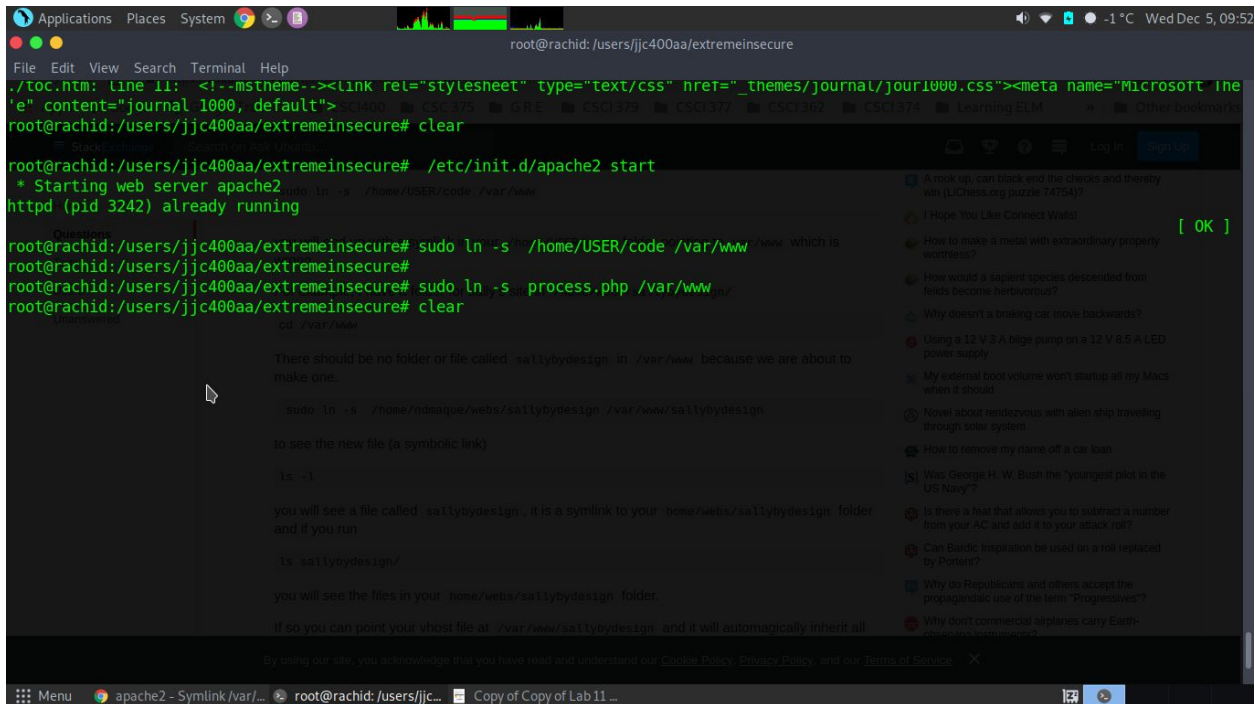
```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help

Last login: Tue Dec 4 21:43:56 2018 from users.isi.deterlab.net
jjc400aa@rachid:~$ sudo apt-get install apache2 php5
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common
  libapache2-mod-php5 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap php5-cli php5-common ssl-cert
Suggested packages:
  apache2-doc apache2-suexec apache2-suexec-custom php-pear php5-suhosin
  openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common
  libapache2-mod-php5 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap php5 php5-cli php5-common ssl-cert
0 upgraded, 14 newly installed, 0 to remove and 0 not upgraded.
Need to get 9,838 kB of archives.
After this operation, 25.0 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://scratch/ubuntu/ precise/main libapr1 amd64 1.4.6-1 [89.6 kB]
Get:2 http://scratch/ubuntu/ precise/main libaprutil1 amd64 1.3.12+dfsg-3 [74.6 kB]
Get:3 http://scratch/ubuntu/ precise/main libaprutil1-dbd-sqlite3 amd64 1.3.12+dfsg-3 [10.4 kB]
Get:4 http://scratch/ubuntu/ precise/main libaprutil1-ldap amd64 1.3.12+dfsg-3 [8,044 B]
Get:5 http://scratch/ubuntu/ precise-updates/main apache2.2-bin amd64 2.2.22-1ubuntu1.11 [1,345 kB]
Get:6 http://scratch/ubuntu/ precise-updates/main apache2-utils amd64 2.2.22-1ubuntu1.11 [92.2 kB]
Get:7 http://scratch/ubuntu/ precise-updates/main apache2.2-common amd64 2.2.22-1ubuntu1.11 [228 kB]
Get:8 http://scratch/ubuntu/ precise-updates/main apache2-mpm-prefork amd64 2.2.22-1ubuntu1.11 [2,412 B]
Get:9 http://scratch/ubuntu/ precise-updates/main apache2 amd64 2.2.22-1ubuntu1.11 [1,490 B]
Get:10 http://scratch/ubuntu/ precise-updates/main php5-common amd64 5.3.10-1ubuntu3.26 [1.778 kB]
```

```
Applications Places System root@rachid: /users/jjc400aa/extremeinsecure
File Edit View Search Terminal Help

_borders feedback_submitted.htm index.htm PointsHere products se
arch.htm _themes _vti_pvt
_derived fpclass news.htm _private products_files se
arch_results.htm toc.htm
root@rachid:/users/jjc400aa/extremeinsecure# ln -sv /users/jjc400aa/extreme
insecure
`./extremeinsecure' -> `/users/jjc400aa/extremeinsecure'
root@rachid:/users/jjc400aa/extremeinsecure# ls
extremeinsecure fpclass news.htm _private produ
cts_files search_results.htm toc.htm
_borders feedback.htm images _overlay process.php produ
cts.htm services.htm _vti_cnf
_derived feedback_submitted.htm index.htm PointsHere products searc
h.htm _themes _vti_pvt
root@rachid:/users/jjc400aa/extremeinsecure# ln -sv /users/jjc400aa/extreme
insecure
ln: failed to create symbolic link `./extremeinsecure': File exists
root@rachid:/users/jjc400aa/extremeinsecure#
```





```
root@rachid: /users/jjc400aa/extremeinsecure
./toc.htm: line 11: <!--mstheme--><link rel="stylesheet" type="text/css" href="_themes/journal/jour1000.css"><meta name="Microsoft The
'e" content="journal 1000, default">
root@rachid: /users/jjc400aa/extremeinsecure# clear

root@rachid: /users/jjc400aa/extremeinsecure# /etc/init.d/apache2 start
* Starting web server apache2
httpd (pid 3242) already running

root@rachid: /users/jjc400aa/extremeinsecure# sudo ln -s /home/USER/code /var/www /www
root@rachid: /users/jjc400aa/extremeinsecure#
root@rachid: /users/jjc400aa/extremeinsecure# sudo ln -s process.php /var/www
root@rachid: /users/jjc400aa/extremeinsecure# clear
```

2.3.1 XSS

I was able to load the localhost files on my machine via adding the conf file to the var/www directory and was able to use elinks  
<http://localhost/XSS/setgetcookie.htm> and elinks  
<http://localhost/XSS/malURL.htm>

What I found inside was a form to fill out a username, password, and to set a cookie for the session as well as submitting username. An interesting aspect of submitting a username within this field is the POST data shows a username and password= in clear text.

For the Malicious URL, I found that the link is attempted to be overwritten in an attempt to override a legitimate website with a malicious url. The mouseover attack fails due to the stripping of data, however in an earlier browser hovering my mouse over the link will indeed trigger the malicious url.

2.3.2 Server-side scripting attacks

For the sample htm request I inputted this command and ended up with "http://localhost/XSS/setgetcookie.htm?username="onMouseOver="window.stat us='http://www.localhost/XSS/../../netstat;return true" onMouseOut"window.status="";return true or something of the sort. In theory this url should work to traverse backwards via the setgetcookie.htm file when passed as a parameter to the sample.htm however due to my usage of elinks I suspect mouseOver to not parse correctly in a CLI environment.

## 2.4 Mail security

```
jennifer@jennifer-VirtualBox: ~
jennifer@jennifer-VirtualBox:~$ sudo apt-get install gnupg
[sudo] password for jennifer:
Sorry, try again.
[sudo] password for jennifer:
Sorry, try again.
[sudo] password for jennifer:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  gnupg-curl gnupg-doc parcimonie
The following packages will be upgraded:
  gnupg
1 upgraded, 0 newly installed, 0 to remove and 688 not upgraded.
Need to get 626 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 gnupg amd64 1.4.20-1ubuntu3.3
[626 kB]
Fetched 626 kB in 1s (411 kB/s)
(Reading database ... 172476 files and directories currently installed.)
Preparing to unpack .../gnupg_1.4.20-1ubuntu3.3_amd64.deb ...
Unpacking gnupg (1.4.20-1ubuntu3.3) over (1.4.20-1ubuntu3) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for install-info (6.1.0.dfsg.1-5) ...
Setting up gnupg (1.4.20-1ubuntu3.3) ...
jennifer@jennifer-VirtualBox:~$ gpg --gen-key
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: keyring '/home/jennifer/.gnupg/secring.gpg' created
gpg: keyring '/home/jennifer/.gnupg/pubring.gpg' created
Please select what kind of key you want:
(1) RSA and RSA (default)
(2) RSA and Elgamal
```

```
jennifer@jennifer-VirtualBox: ~
jennifer@jennifer-VirtualBox:~$ gpg --gen-key
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 1024
Requested keysize is 1024 bits
Please specify how long the key should be valid.
  0 = key does not expire
  <n> = key expires in n days
  LibreOfficeImpress xpires in n weeks
  <n>m = key expires in n months
  <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
  "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Jennifer
Email address: jennifer.garcia5@jjay.cuny.edu
Comment: Hello
You selected this USER-ID:
  "Jennifer (Hello) <jennifer.garcia5@jjay.cuny.edu>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

passphrase not correctly repeated; try again.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.

Not enough random bytes available. Please do some other work to give
the OS a chance to collect more entropy! (Need 247 more bytes)
.+++++
+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
Amazon
.....+++++
+++++
gpg: /home/jennifer/.gnupg/trustdb.gpg: trustdb created
gpg: key 90177A28 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
pub 1024R/90177A28 2018-12-05
```

```

uid          Jennifer (Hello) <jennifer.garcia5@jjay.cuny.edu>
sub          1024R/9675F442 2018-12-05

jennifer@jennifer-VirtualBox:~$ gpg --export [uid] -o FILENAME
gpg: WARNING: nothing exported
jennifer@jennifer-VirtualBox:~$ GPG --export [uid] -o FILENAME
GPG: command not found
jennifer@jennifer-VirtualBox:~$ gpg --export [uid] -o UNTITLED DOCUMENT
gpg: WARNING: nothing exported
jennifer@jennifer-VirtualBox:~$ touch FILENAME
jennifer@jennifer-VirtualBox:~$ gpg --export [uid] -o FILENAME
gpg: WARNING: nothing exported
jennifer@jennifer-VirtualBox:~$ gpg --export [Jennifer (Hello)] -o FILENAME
bash: syntax error near unexpected token `('
jennifer@jennifer-VirtualBox:~$ gpg --export [Jennifer] -o FILENAME
gpg: WARNING: nothing exported
jennifer@jennifer-VirtualBox:~$ gpg --export [jennifer.garcia5@jjay.cuny.edu] -o FI
LENAME
gpg: WARNING: nothing exported
jennifer@jennifer-VirtualBox:~$ gpg --export [Jennifer <jennifer.garcia5@jjay.cuny.
edu>] -o FILENAME
bash: jennifer.garcia5@jjay.cuny.edu: No such file or directory
jennifer@jennifer-VirtualBox:~$ gpg --export [<jennifer.garcia5@jjay.cuny.edu>] -o
FILENAME
bash: jennifer.garcia5@jjay.cuny.edu: No such file or directory
jennifer@jennifer-VirtualBox:~$ gpg --export [FILENAME] -o FILENAMEgpg: WARNING: no
thing exported
jennifer@jennifer-VirtualBox:~$ gpg --export [Jennifer] -o FILE.pdf
gpg: WARNING: nothing exported
jennifer@jennifer-VirtualBox:~$ gpg --export -a "Jennifer" > public.key
jennifer@jennifer-VirtualBox:~$ gpg --import public.key
gpg: key 90177A28: "Jennifer (Hello) <jennifer.garcia5@jjay.cuny.edu>" not changed
gpg: Total number processed: 1

```

### 3 Word Problems

1. To what extent do utilities like NoScript protect against cross-site-scripting attacks?

No script protect against cross-site-scripting attacks by stripping the data required to trigger scripts from nontrusted user submitted scripts such as alert javascripts and others. It does this by removing the ability to run scripts on sites automatically at site load time.

2. What would you improve in NoScript?
  - a. Some improvements to be made in NoScript are to only allow temporary script usage on a site and to also make third party domains and trackers available to perform NoScript restrictions on at default.
3. What file permissions, if any, would prevent attacks as described in the web sections?

- a. Removing the chmod 777 permission if present this will create easy attack surface allowing for read write and execute permissions. This approach is extremely unsafe and should never be done on any web servers particularly front facing ones.
  - b. Instead opt in for chmod 755 for any directories and chmod 644 for files and their required dependencies.
- 4. How would you break the security provided by GPG?
  - a. In order to break it I would use a dictionary attack to get the secret key or to get the email password and get the key through there.