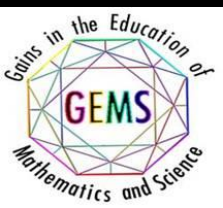




U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND DATA & ANALYSIS CENTER

CAPTURE THE FLAG 2.0

Dr. Oscar Perez, Stephen Cruz, Herandy Vazquez,
Juan Ulloa, Andrew Clanan, Salvador Melendez





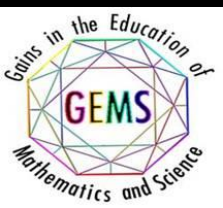
CODE OF ETHICS



- This workshop is intended to be an education tool to make students aware of the risks of electronic communications.
- The future of electronic communications has to be in charge of a cyber police with the highest standards of ethics.
- **What is ethics? moral principles that govern a person's behavior or the conducting of an activity. Always remember:**



**WITH
GREAT
POWER COMES
GREAT
RESPONSIBILITY**





WORKSHOP OBJECTIVES



Today, you will learn about:

✓ ***Social Engineering***

* *Dumpster Diving*

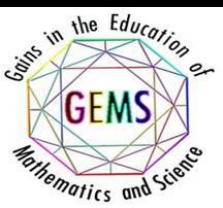
✓ ***Encryption***

* *Encoding/Decoding (e.g. steganography)*

* *Password Auditing (e.g. john)*

✓ ***Access Control***

* *User/Admin Level (e.g. ssh)*





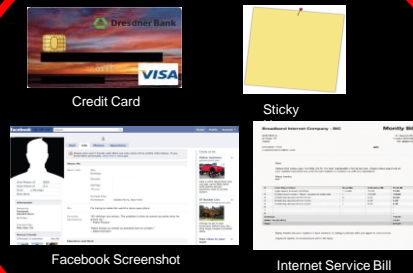
OVERVIEW



Download and
Run Python Script



Dumpster Diving



Password Auditing



Steganography



Quiz & Survey



Access Control



DUMPSTER DIVING



WHAT?

Social Engineering technique used to gather Personal Identifiable Information (PII).

HOW?

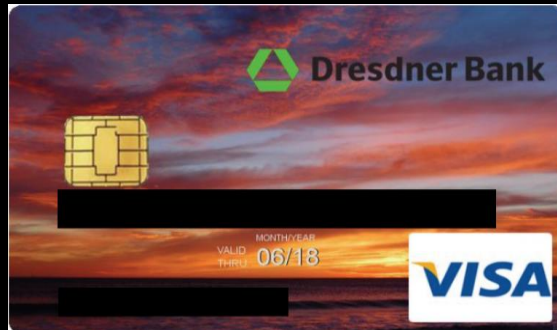
Looking into the trash, websites, mailboxes, etc. and putting pieces together.

EXAMPLES OF DOCUMENTS:

Credit Card, Electricity Bill, Facebook Profile, Paper Notes.



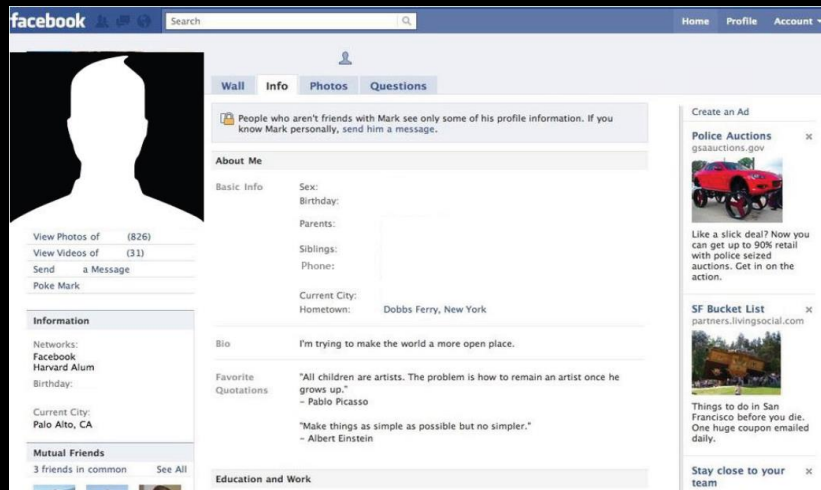
DUMPSTER DIVING



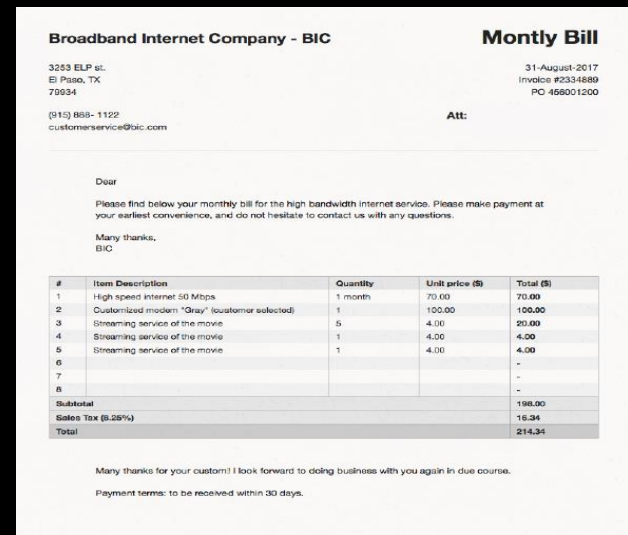
Credit Card



Sticky Note



Facebook Screenshot



Internet Service Bill



DUMPSTER DIVING



- By performing Dumpster Diving, you will get important personal identifiable information (PII) of a person.
- Write down on a paper the following information of the person you are investigating:

User: _____ (hint: is the first part of the email address, everything before the @)

PIN: _____

Favorite Movie: _____

Country Code: _____ (hint: is NOT 915, is a 1-digit or 2-digit number)

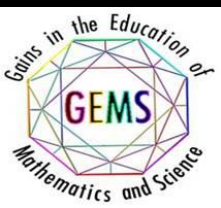
Year of Birth: _____

Dumpster Diving Command

```
pi@raspberrypi: ~
```

```
File Edit Tabs Help
```

```
pi@raspberrypi:~ $ python3 dumpster_diving.py
```





DUMPSTER DIVING



4 Tabs → 1) Credit Card, 2) Post-It, 3) Facebook Profile, and 4) Monthly Bill

Credit Card Post-It Facebook Screenshot Monthly Bill

0715 539 2950

REBECCA aBank Ide

4916 8 VALID THRU 10/17 VISA

Drag & Drop the pieces to solve the puzzle



PASSWORD AUDITING



WHAT?

Is the process of guessing a password by hashing different words and comparing those hashes against the hash to be guessed.

HOW?

Using John The Ripper (john for short)

Command:

`john --wordlist=cracking_wordlist.txt shadow`

John The Ripper

List of possible dictionary words to hash and compare against the hashes inside the "shadow" file

File that contains the hashes to crack

Hashed Password you are trying to guess		Possible Passwords
5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8		
No	19a6dbf1bf05b16195eaf24f1fa43efdc3d317dd	michael
No	2a72a1f522016f4fd660fd19aa415ac5c3d33568	123456
No	4145abd8e29dfe738096b117c771c538c3d319bb	superman
Equal !	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8	password
	c6e173c0f381158c32f787e1d5c67530c3d32339	qwerty
	e69177b3636633b524162be07573abeec3d31fc0	letmein

This password matches the hash!

Possible Hashes



PASSWORD AUDITING



Wordlist

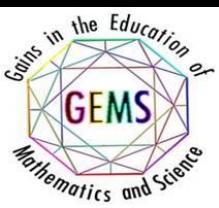
```
cracking_wordlist - Notepad
File Edit Format View Help
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
```

Shadow File

```
shadow - Notepad
File Edit Format View Help
jpalmer:$1$x0WwV2.$htuTSPjGfRveNDxnjGh2U0:18820:0:99999:7:::
spaterson:$1$5XAY/RuQ$ugPkCqZwnZk2Ks4Q5TfGQ.:18820:0:99999:7:::
rchesterton:$1$X.AU7sek$Aexzbdv9s1g2H.4NTsn.m.:18820:0:99999:7:::
ikendal:$1$0hHJx93t$6pdt0E5QpNI5IB4QaAI/c.:18820:0:99999:7:::
vthornton:$1$SC5WZxzk$py0nc1LbszWdYG701Qzmb/:18820:0:99999:7:::
swarren:$1$zlos79oe$Zt7v873HKWli9bHh1tAGV1:18820:0:99999:7:::
agibbs:$1$fbVC05xq$yoeNTpwxr1EYXk319knCi0:18820:0:99999:7:::
jmathews:$1$MJ10.Up2$1cXJCe/UERTmOhpQ76NVo/:18820:0:99999:7:::
lderrick:$1$b9GFOQLy$/97bggGgMIMsZexUyZUJL/:18820:0:99999:7:::
dotis:$1$Rc.RMMVP$MiDioBBv7J4nxshStw5OZ1:18820:0:99999:7:::
eowen:$1$9Hk5WB99$G4QZHK6MESTzP1b1.qQVR0:18820:0:99999:7:::
gbecker:$1$fkB9CvDK$0t7w1UzwH1/duu0WS/qBV1:18821:0:99999:7:::
```

john Command

```
pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~ $ john --wordlist=cracking_wordlist.txt shadow
```

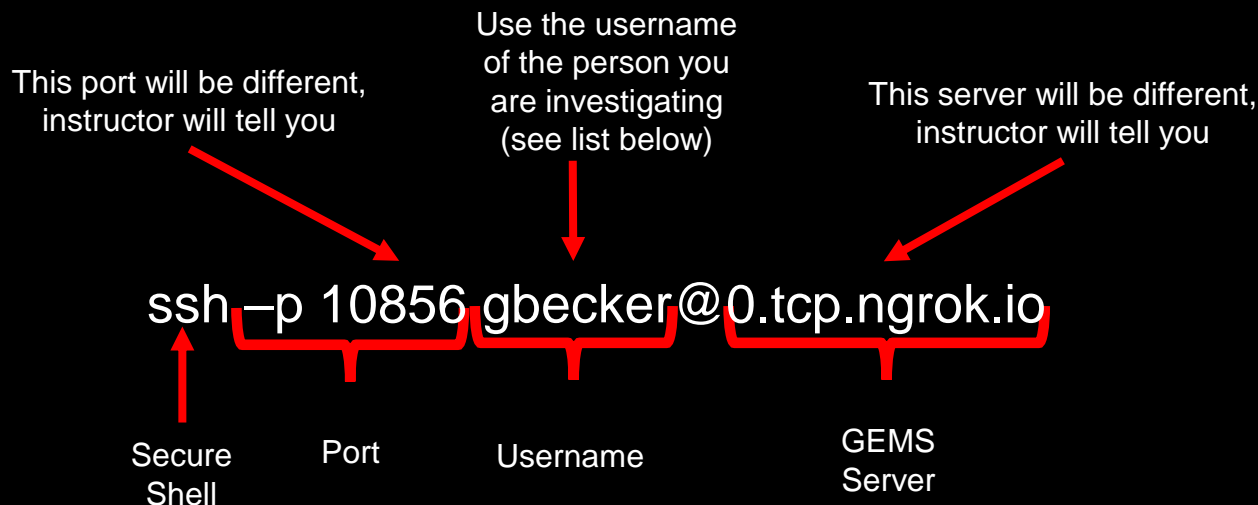




ACCESS CONTROL



- Establish a SSH connection to the GEMS server:

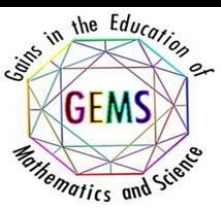


Possible Usernames (check which one belongs to the person your are investigating):

- | | |
|---------------|------------|
| - gbecker | - swarren |
| - apalmer | - agibbs |
| - spaterson | - jmathews |
| - rchesterton | - lderrick |
| - ikendal | - dotis |
| - vthornton | - eowen |

Example Command:

```
File Edit Tabs Help
pi@raspberrypi:~ $ ssh -p 10856 gbecker@0.tcp.ngrok.io
```





ACCESS CONTROL



- After you establish the SSH connection, list files using ls
- If you find the file “secret_message.txt”, use the cat command to see its contents
- Write down the name of the image with the secret message, you will need it

```

gbecker@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~ $ ssh -p 10856 gbecker@0.tcp.ngrok.io
Warning: Permanently added the ECDSA host key for IP address '[3.17.7.232]:10856' to the list of known hosts.
gbecker@0.tcp.ngrok.io's password:
Linux raspberrypi 4.19.97-v7l+ #1294 SMP Thu Jan 30 13:21:14 GMT 2020 armv7l

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul 13 15:24:23 2021 from ::1

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
a new password.

gbecker@raspberrypi:~ $ ls
secret_message.txt
gbecker@raspberrypi:~ $ cat secret_message.txt
My secret message is hidden in [redacted].png
gbecker@raspberrypi:~ $

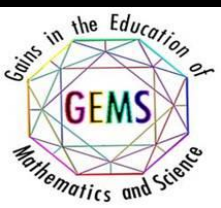
```

ssh connection

List files

See contents of file

Name of image with secret message





STEGANOGRAPHY

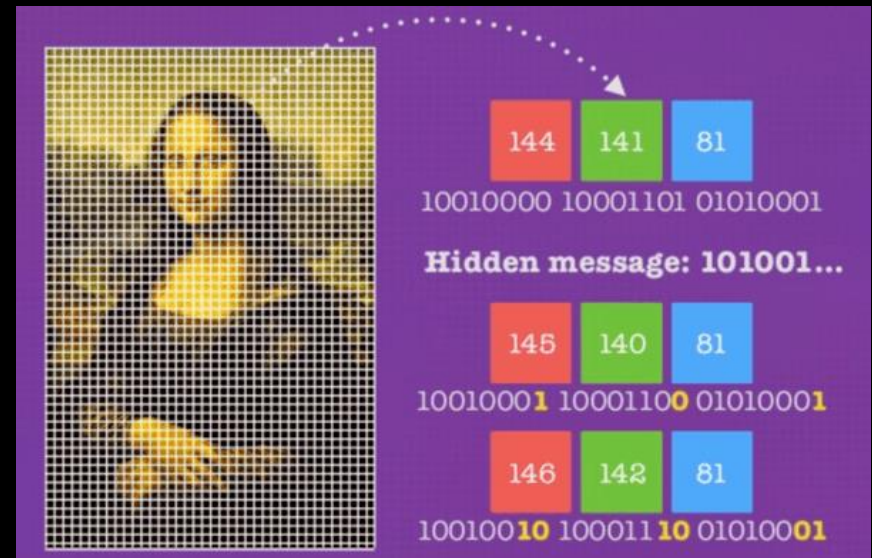


What?

- A technique used to hide data within an ordinary file (e.g. image, sound, text, etc.) to keep information secret from a naked eye.
- Steganography can be combined with Encryption to provide more security

Steganography on Images.

- Each pixel in the image has colors defined in RGB (Red, Green, Blue) format → Color intensity ranges from 0 to 255



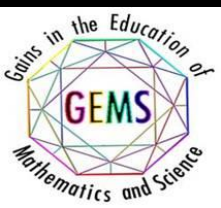


STEGANOGRAPHY



- You will be prompted if you want to “Encode” or “Decode”.
 - Type “1” or “E” or “e” to Encode
 - Type “2” or “D” or “d” to Decode
- Type 2, hit enter, then type the NUMBER between brackets, hit enter
- Write down the secret message that belongs to the person you are investigating.

```
pi@raspberrypi: ~  
File Edit Tabs Help  
pi@raspberrypi:~ $ python3 steganography.py  
Hello!  
Encode or Decode Image? (Type 1 or E to Encode. Type 2 or D to Decode)  
2  
  
Available images to decode:  
[0] new_image_712.png  
[1] new_image_717.png  
[2] new_image_480.png  
[3] new_image_204.png  
[4] new_image_610.png  
[5] new_image_286.png  
[6] new_image_108.png  
[7] new_image_683.png  
[8] new_image_170.png  
[9] new_image_318.png  
[10] new_image_311.png  
[11] new_image_591.png  
  
From the list above, which image do you want to decode? Enter the number between  
n []: 6
```





ACCESS CONTROL



- Establish a SSH connection to the GEMS server

This port will be different,
instructor will tell you

Use pi as
username

This server will be different,
instructor will tell you

ssh -p 10856 pi@0.tcp.ngrok.io

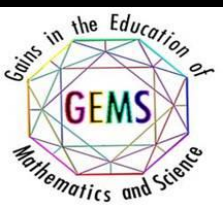
Secure Shell Port Username GEMS Server

Example Command:

```
pi@raspberrypi: ~/gems_2021
```

```
File Edit Tabs Help
```

```
pi@raspberrypi:~ $ ssh -p 10856 pi@0.tcp.ngrok.io
```





ACCESS CONTROL



- After you establish the SSH connection, cd into “gems_2021” folder, list files with ls, and look for your name.
- Use pico to edit the file with your name.

```

pi@raspberrypi: ~/gems_2021
File Edit Tabs Help
pi@raspberrypi:~ $ ssh -p 10856 pi@0.tcp.ngrok.io
Warning: Permanently added the ECDSA host key for IP address '[3.134.125.175]:10856' to the list of known hosts.
pi@0.tcp.ngrok.io's password:
Linux raspberrypi 4.19.97-v7l+ #1294 SMP Thu Jan 30 13:21:14 GMT 2020 armv7l

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul 13 15:24:02 2021 from ::1

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi:~ $ cd gems_2021/
pi@raspberrypi:~/gems_2021 $ ls
alejandros_hernandez  drevan_padilla_martinez  lascrucses  orion_baker
andreas_shams         elpaso                  lauren_to   ridley_dean
angel_corral          iris_hernandez          muriel_cain  rodrigo_perez
benedek_szalai        isaiah_romero           nathan_perez salvador_melendez
brayden_allison       jaden_hewston           nicolas_gonzalez savannah_skow
claudio_corral        kase_deruyter           noah_contreras uzeah_netto
delilah_vega          katherine_baer          olivia_leon
pi@raspberrypi:~/gems_2021 $ pico salvador_melendez

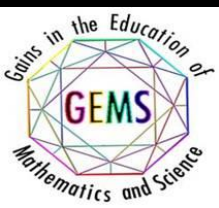
```

ssh connection

Change directory to “gems_2021”

List files and look for your name

Edit your file with pico





SURVEY



– Answer the Quiz & Survey.

```

GNU nano 3.2          survey.txt

***Please answer the following questions and save the file:

1.- From the person you investigated, please provide the following information:
User (hint: is the first part of the email address, everything before the @):
PIN:
Favorite Movie:
Country Code (hint: is NOT 915, is a 1-digit or 2-digit number):
Year of Birth:

2.- What is the password of the person you investigated and that you cracked using John the Ripper?

3.- What is the command that you've used to crack/guess the passwords using John The Ripper?

4.- What python script did you use to decode the image with a secret message?

5.- What is the secret message that you decoded from the image?

6.- What python script did you use to solve the puzzles with Personal Identifiable Information (PII)?

7.- Tell us something you liked about the GEMS program.

8.- Tell us something you did NOT like about the GEMS program.

9.- Would you recommend the GEMS program to a friend?

10.- How can we improve the quality of the GEMS program?

11.- From 1 to 10, what score will you give to the GEMS program? (1 is the lowest score, 10 is the highest score)

12.- We will send you a Certificate of Participation for GEMS II, please provide us the following information:
What's your name:
What's your email address:
Did you attend GEMS in El Paso or Las Cruces?

THANK YOU!!!
GEMS

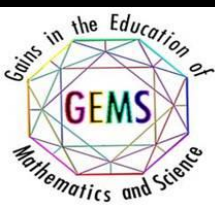
^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify     ^C Cur Pos     ^M-U Undo
^X Exit          ^R Read File    ^_ Replace      ^_ Uncut Text   ^T To Spell    ^_ Go To Line   ^M-E Redo
  
```

Answer
the Quiz

Answer
the Survey

Fill out your name and
email, we will send you a
certificate of completion

**DON'T FORGET
TO SAVE THE
FILE WITH YOUR
ANSWERS!!!**





SURVEY



- Move your file to “elpaso” or “lascruces” (depending on where you are at).

Example Command:

```
pi@raspberrypi:~/gems_2021 $ mv salvador_melendez elpaso/
```

- Verify if your file was moved by using cd and ls (as shown below), then exit the SSH connection by typing “exit”.

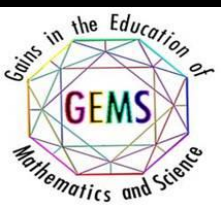
Example Command:

```
pi@raspberrypi:~/gems_2021 $ mv salvador_melendez elpaso/
pi@raspberrypi:~/gems_2021 $ cd elpaso/
pi@raspberrypi:~/gems_2021/elpaso $ ls
salvador_melendez
pi@raspberrypi:~/gems_2021/elpaso $ exit
logout
Connection to 0.tcp.ngrok.io closed.
pi@raspberrypi:~ $
```

Change directory to
“elpaso” or “lascruces”

List files and look
for your name

Exit SSH connection





DOWNLOAD FILES



- Ready for the challenge?
- Open a terminal and download all the needed scripts from the internet by using the following command:

```
wget https://raw.githubusercontent.com/salvadmelenandez/gems2021/main/gems_setup.py
```

Example Command:

pi@raspberrypi: ~

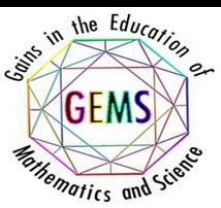
File Edit Tabs Help

```
pi@raspberrypi:~ $ wget https://raw.githubusercontent.com/salvadmelenandez/gems2021/main/gems_setup.py
```

- Run the python script by typing:

```
python3 gems_setup.py
```
- Wait until you see a message saying: “You are all set!”
- Start the challenge with Dumpster Diving (slide 7). Follow slides 7 through 18. These slides are in your Raspberry Pi (/home/pi/challenge.pdf)
To open the slides, open a terminal and type the following command:

```
xdg-open challenge.pdf
```





CONTACT INFORMATION



Salvador Melendez, Ph.D.

UNCLASSIFIED email: salvador.melendez3.civ@mail.mil

