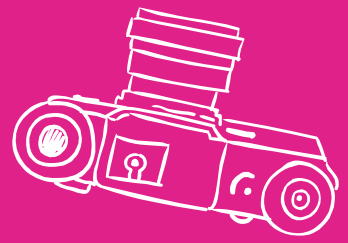
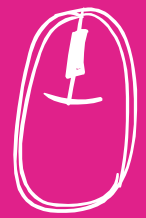
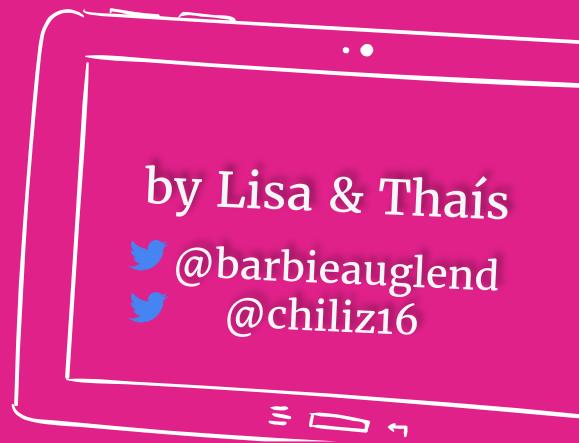




Pwntools

@PyLadies Munich – January 2020

by Lisa & Thaís
@barbieauglend
@chiliz16


DISCLAIMER

The opinions and positions expressed are ours only and do not represent the views of any current or previous employer, including Intel Corporation or its affiliates.

This presentation has no intention to advertise or devalue any current or future technology.




Agenda

1. CTF? Hacking? Pwn?
2. Binary exploitation 101
3. Pwntools ftw

Picture added by KateKicksAss on tumblr

CTF! HACKING! PWN!

a short intro into the world of cyber security

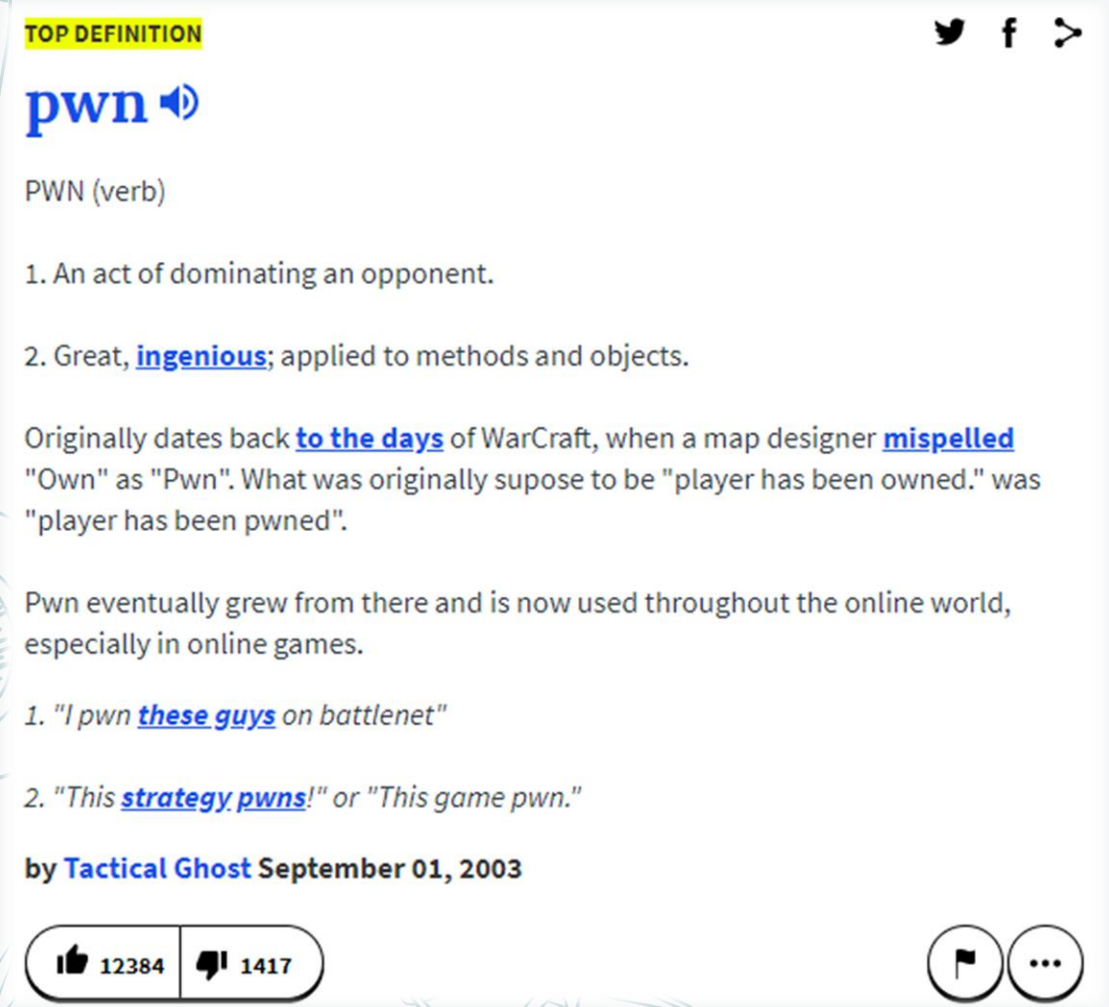
CTF> echo "Capture the flag"

- Gamified approach to the core skills needed in IT Security

- A way to learn new technologies, be creative and play around with them
- You can use it as a kickstart motivation to look into something
- Forces you to look deeper (in order to hack something, it's good to know it in-depth)

By chiliz

PWN> ECHO "DWAG, YOU OWN IT!"



TOP DEFINITION

pwn

PWN (verb)

1. An act of dominating an opponent.

2. Great, **ingenious**; applied to methods and objects.

Originally dates back **to the days** of WarCraft, when a map designer **mispelled** "Own" as "Pwn". What was originally supose to be "player has been owned." was "player has been pwned".

Pwn eventually grew from there and is now used throughout the online world, especially in online games.

*1. "I pwn **these guys** on battlenet"*

*2. "This **strategy pwns**!" or "This game pwn."*

by Tactical Ghost September 01, 2003

12384 1417

"I'm in" - That's what hackers say in movies when they enter a system.

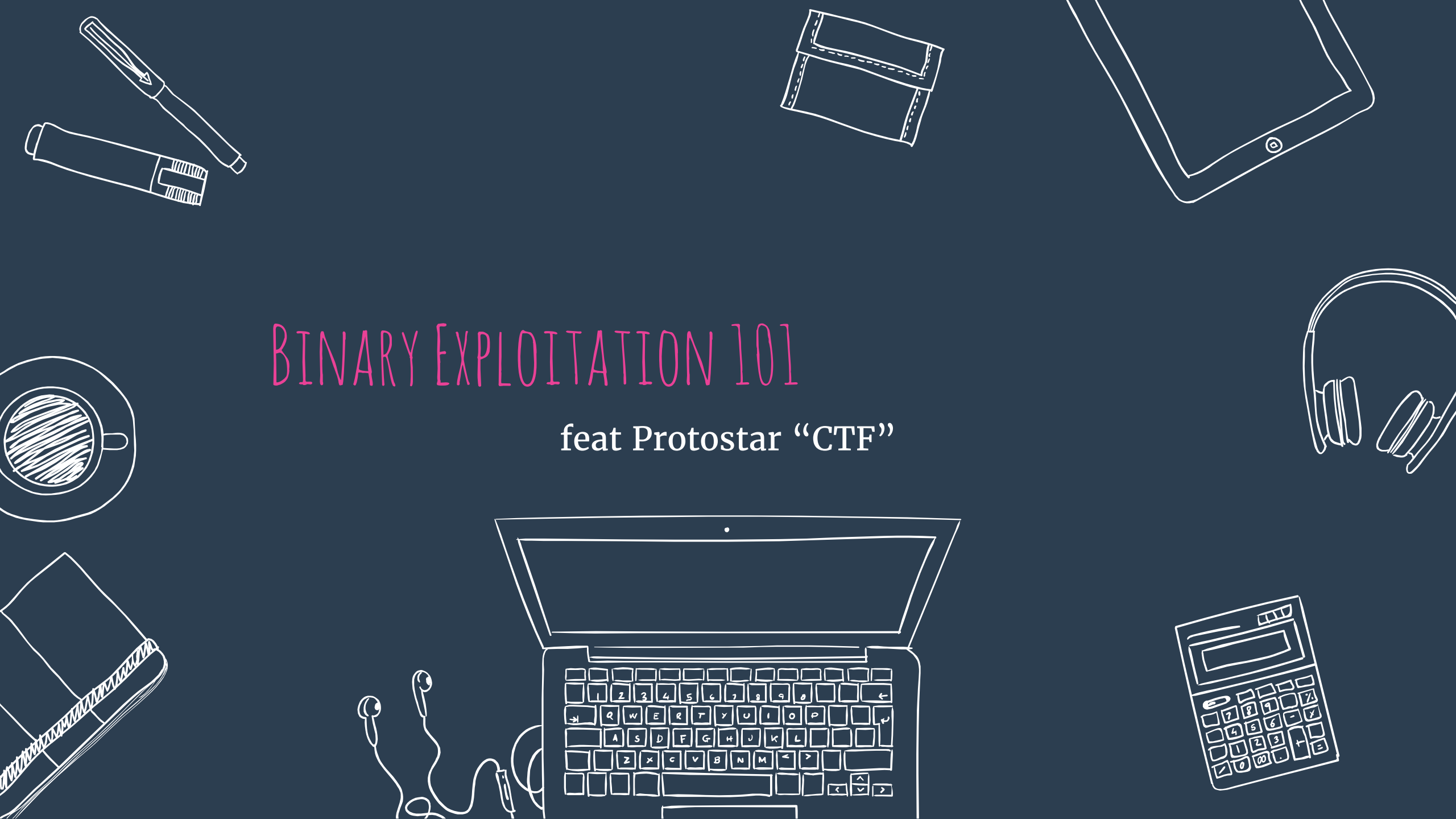
"pwned!" is the 'cool' way to say that - "owning" in the sense of conquered to gain ownership.

By chiliz

Source: https://www.urbandictionary.com/define.php?term=pwn

Binary Exploitation 101

feat Protostar “CTF”



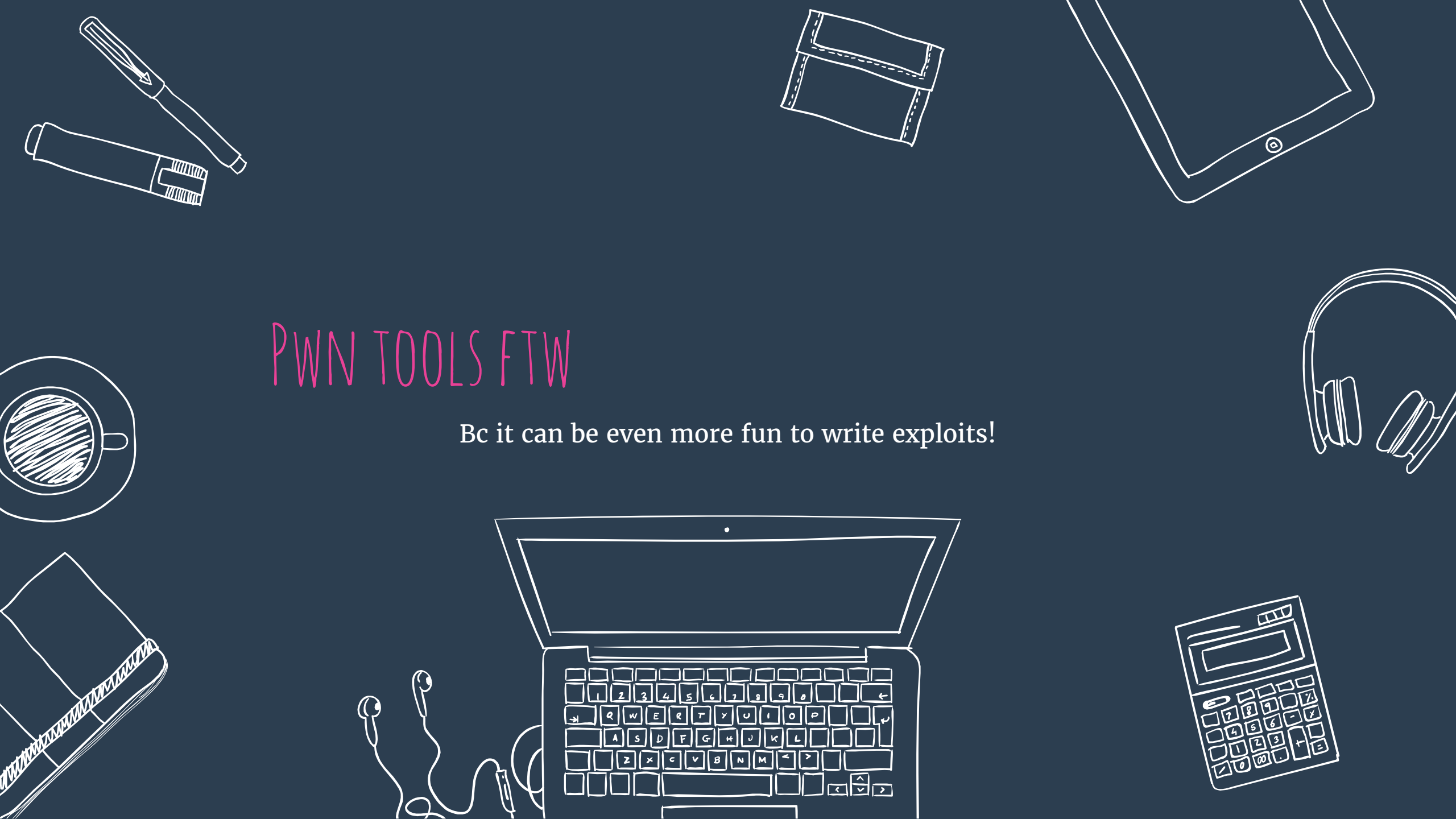
PYLADIES> ./PROTOSTAR

```
$ pyladies> ./bin_expl --help

"Binary exploitation is the process of subverting a compiled
application such that it violates some trust boundary in a way that
is advantageous to you. The most common way of doing it is
known as memory corruption, where we can hijack the control
flow of the application and run your own code."

$ pyladies> cat protostar/stack0.c

#include <stdlib.h>
#include <unistd.h>
```

https://exploit-exercises.lains.space/protostar/
https://linux.die.net/man/3/gets

Pwn tools ftw

Bc it can be even more fun to write exploits!



Installing pwntools

```
apt-get update
apt-get install python3 python3-pip python3-dev git libssl-dev libffi-dev build-essential
python3 -m pip install --upgrade pip
python3 -m pip install --upgrade git+https://github.com/Gallopsled/pwntools.git@dev3
```

Source: https://github.com/Gallopsled/pwntools

In MacOS you can also use brew :D

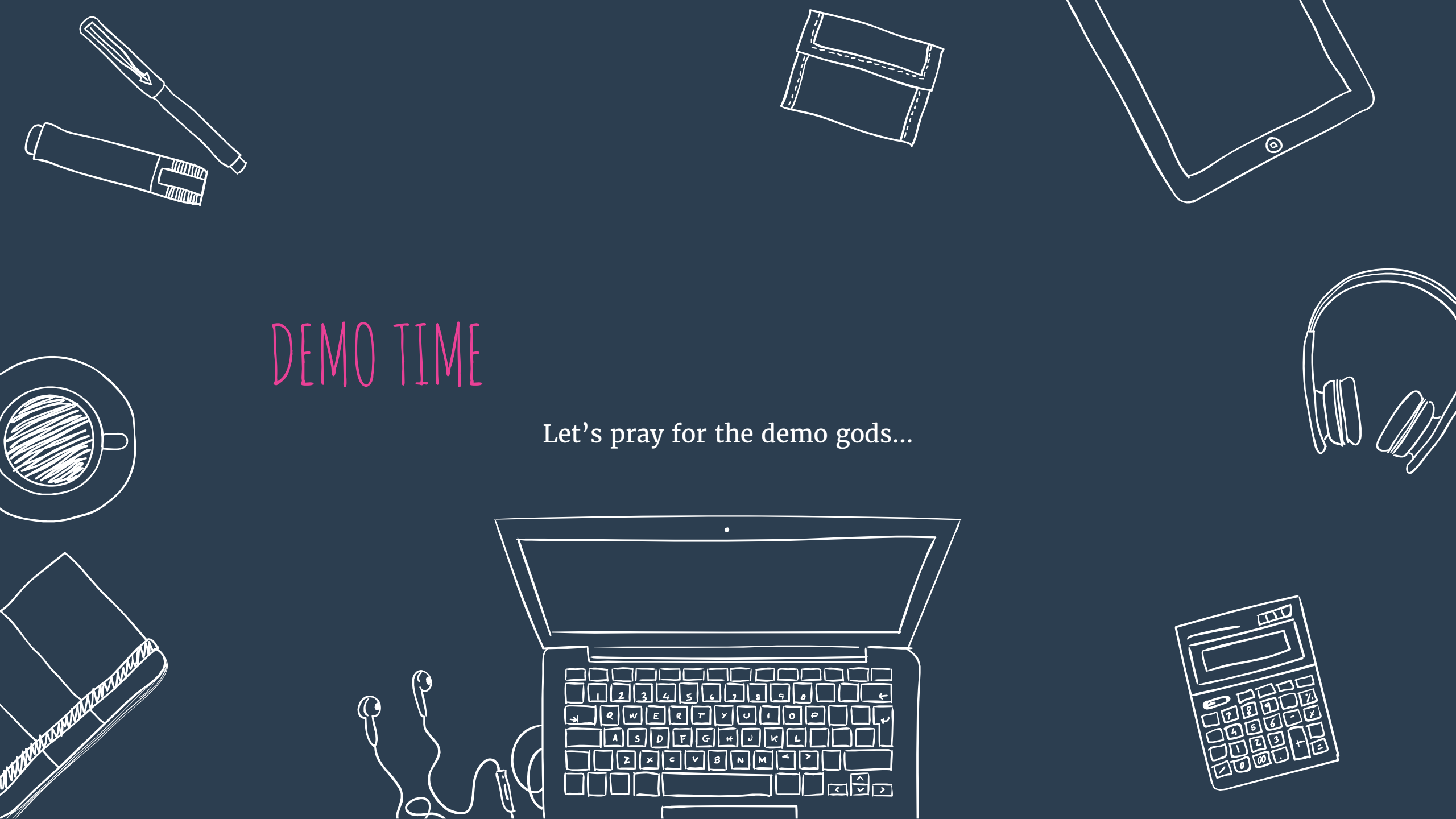
First steps w/ pwntools

```
#!/usr/bin/python3

import sys
from pwn import *

BINARY_NAME = 'changeme'

#FILLBUF = XX
def pwn_do(r):
    pause()
    #payload = b"A" * FILLBUF
    #payload +=  ...

if __name__ == "__main__":
    if len(sys.argv) > 2:
        r = remote(sys.argv[1], sys.argv[2])
        pwn_do(r)
    else:
        r = process(BINARY_NAME)
        pwn_do(r)
```

```
# sends data + EOL
io.sendline(payload)

# receives byte sequence terminated by EOL
io.recvline()

# Launches a GDB server and attaches GDB to it
gdb.debug(BINARY_NAME)

# returns a at most length elements over
# a De Bruijn sequence
cyclic(INT)

# Calculates the position of a substring
# into a De Bruijn sequence
cyclic_find($ADDR)

# Encapsulates information about an ELF file.
binary=ELF('/usr/lib/libc-2.17.so')

# Searches the address for the specified string.
binary.search('/bin/sh')
```

DEMO TIME

Let’s pray for the demo gods...



First steps w/ pwntools

How many bytes do we have to write until we reach RIP?

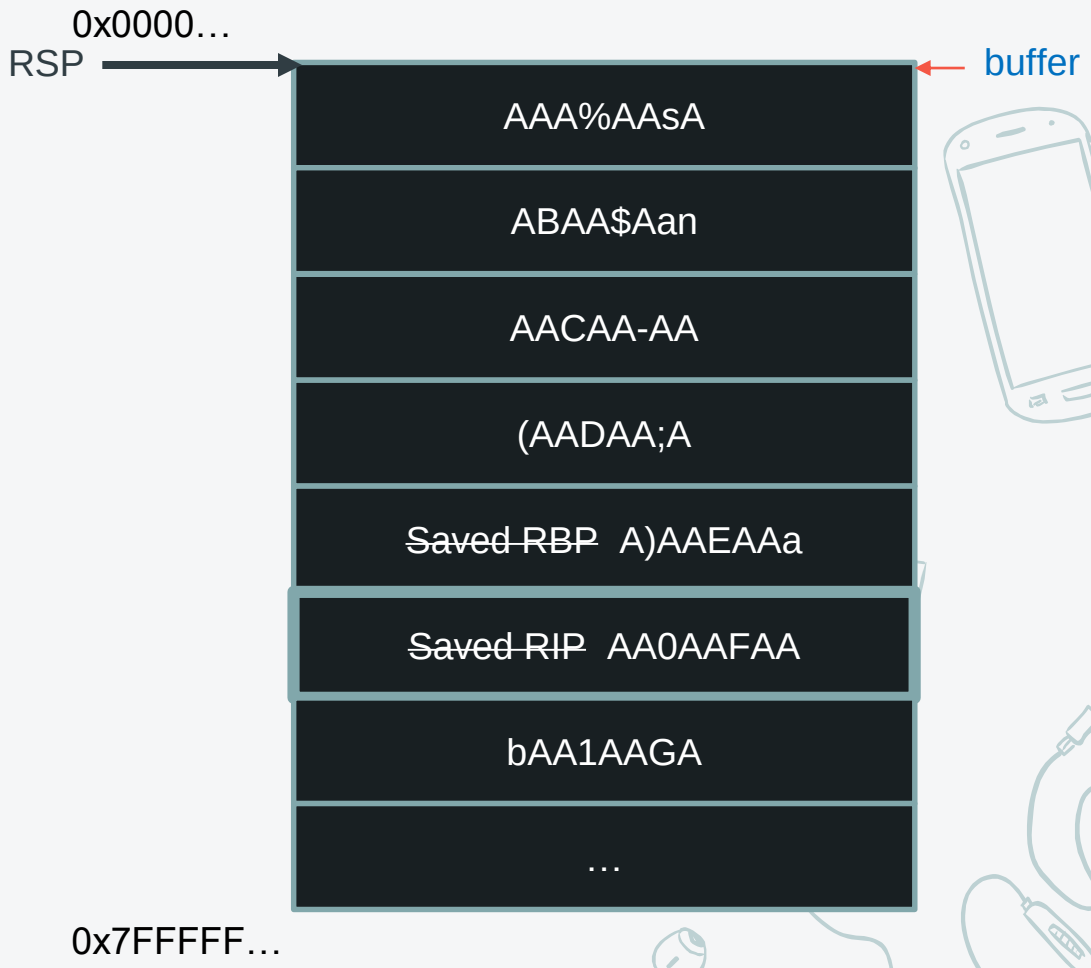
Input - String = 40*"A" + 8*"F"

Program call:

```
>    ./myprogram AA…(A*40)FFFFFFFF
! Buffer Overflow, RIP is now FFFFFFFF
```

First steps w/ pwntools

```
IN[1]: from pwn import *

1. Generate Pattern
   IN[4]: cyclic(60)
                                  AAA%AAsAABAA$AAnAACAA-AA

2. Pattern as input for the program
   gef$ run
   Give me a string that gets you the flag:
                                  AAA%AAsAABAA$AAnAACAA-AA

3.Find the part in the pattern that overwrote RIP
   IN[5]: cyclic_find(b'AAA%AAsAABAA$AAnAACAA-AA')

4. Pwntools internally uses pattern matching for that



AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGA
                                  AA0AAFAA
                                  Match!
                                  Offset: 40
```



PWNED!

Thank u 4 ur ‘AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA’> & ttyl :)

$