HACK ILLINOIS

LITERALLY

SIGPWNY

Outline

- Who are we?
- What is cybersecurity?
- Activity 0 (Breaking into Siebel Center)
- Activity 1 (SQL Injection)

whois sigpwny

- SIGPwny (50+ active, sigpwny.com)
- Thomas Quig (President - quig.dev)
- Nathan Farlow (Office - farlow.dev)

@SIGPwny

https://discord.gg/cWcZ6a9

What is Cybersecurity?

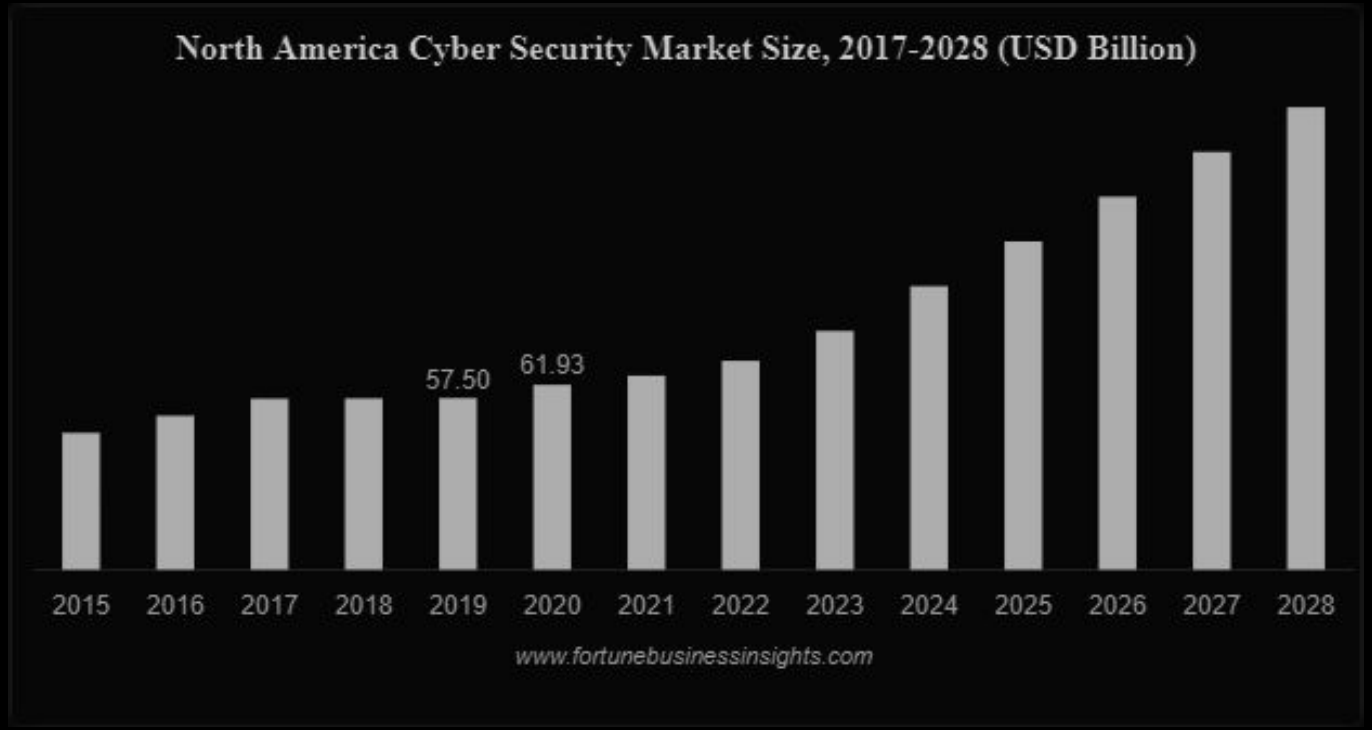
```
4141 4141 4141 4141 4141 4141 4141 4141 | AAAA AAAA AAAA AAAA
4141 4141 4141 4141 4141 4141 4141 4141 | AAAA AAAA AAAA AAAA
4141 4141 4141 4141 4141 4141 4141 4141 | AAAA AAAA AAAA AAAA
4141 4141 4141 4141 4141 4141 4141 4141 | AAAA AAAA AAAA AAAA
4141 4141 4141 4141 4141 4141 4141 4141 | AAAA AAAA AAAA AAAA
```

Security – Basic Information

- What is Computer Security
  - Breaking or protecting technological systems
- Industry is HUGE
  - 61.93 Billion Dollars in North America Alone
  - Expected to be worth 400+ **Billion** by 2030
- Nomenclature
  - Cybersecurity, Infosec, Computer Security, NetSec
  - Hacking
  - Cybercriminals

[1] https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

NA Cybersecurity Market



WARNING before I go any further!

- https://www.law.cornell.edu/uscode/text/18/1030
  - Read it!
- CFAA TLDR
  - Computer Fraud and Abuse Act
  - Attacking “protected” computers
  - Anywhere between a fine and **TWENTY** years in jail.
- If you don’t have EXPLICIT permission to break into it, **DON’T**
- I am NOT a lawyer

Marcus Hutchins, Controversial Hacker who saved the internet, got arrested for past crimes.

I am NOT suggesting, telling, or implying you should actually do these things. If you do them, that’s on you not on me.

That being said

Let’s break into a building after hours

Activity 0

Breaking into Siebel


ONE WAY

Siebel Center

How would you break in after hours?

What are your...

Objectives?

Resources?

What are the...

Targets?

Assumptions?


ONE WAY

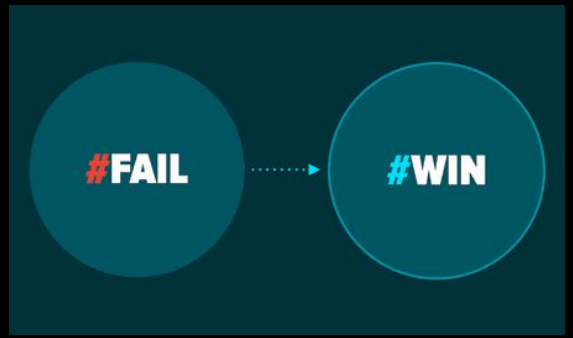
Breaking into Siebel Center (after hours)

- Walk in during the day, stay until close
- Wait for someone to open a door, prop it open.
- Walk in with someone who is already authenticated
- Go up to the door and ask someone to let you in
- Find a door someone left open
- Pretend to be a delivery driver
- Get an authenticated card / key
- Wait for a blackout, hope the door locks fail
- Find an open door on a balcony
- Get a job at Siebel, be given authentication
- Break a window
- Destroy the weak locks on the service entrance
- Run through a wall with a car
- Use an electromagnet to disable the magnetic locks
- Threaten or bribe an employee to let you in

Don’t break in

The adversarial mindset

- How to think when approaching a security situation
- "What would an adversary do?"
- What assumptions exist, and how can you break them?



Isn't this the dumbest image you've seen this week?
(I Googled "Adversarial Mindset" and found this)

Questions?

Activity 1

SQL Injection

SQL Injection

- One of the most common web vulnerabilities in early 2010s
  - Still relevant today
  - Most commonly found in login portals or search functionality on web pages
- Potentially devastating effects
  - Dump user information from database
  - Potential privilege escalation to deface website
- Occurs when hackers can “inject” their own SQL code into the website’s SQL query
- Website creators incorrectly ASSUMED user input was valid data

PHP+SQL Example

```php
<?php
	$username = $_POST['username'];
	$password = $_POST['password'];

	//Actual SQL query is here V
	$query = "SELECT * FROM users WHERE username = '$username' AND password = '$password'";

	$results = $db->query($query);
	$row = $results->fetchArray();

	echo 'Welcome', $row['username'];
?>
```

What can we insert for **$username** and **$password** to make this misbehave?

```
SELECT * FROM users WHERE username = '$username' AND password = '$password'
```


```
SELECT * FROM users WHERE username = 'hello'--' AND password = 'goodbye'
```

```
SELECT * FROM users WHERE username = 'hello'-- ' AND password = 'goodbye'
```

This SQL expression will always log us in as user hello without needing a password!

Limitations

- What if we don’t know the username?
  - Find a `$username` and `$password` which causes the SQL statement to always be true, regardless of username

Quintessential SQL Injection

```
$username = ' OR 1=1--
$password = anything
```

```
SELECT * FROM users WHERE username = '$username' AND password = '$password'
```



```
SELECT * FROM users WHERE username = '' OR 1=1-- AND password = 'anything'
```

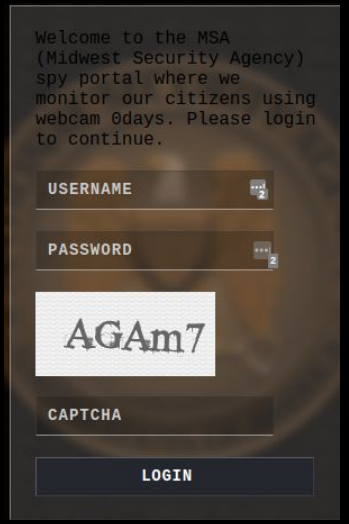


```
SELECT * FROM users WHERE username = '' OR 1=1-- ' AND password = 'anything'
```

This SQL expression will log us in as the first user without a need for a username or password!

Go try for yourself!

http://hackill.sigpwny.com




```
SELECT * FROM users WHERE username = '$username' AND password = '$password'
```

You win if you can find a ‘flag’: sigpwny{...}