Computer Security 101

Presentation By: Thomas Quig

Outline

- whoami
- What is cybersecurity?
- Activity 0 (Breaking into Siebel Center)
- Activity 1 (BOF)
- How to Learn Cybersecurity
- Core Cybersecurity Topics
- Career Paths
- Q & A

whoami

- Thomas Quig (quig.dev)
- UIUC Junior – Computer Science
- SIGPwny
- Network Security (llss.page)
- OSINT
- Pentesting

@Thomas_Quig

@Sonicninja#2238

Email : thomasquig.dev@gmail.com

What is Cybersecurity?

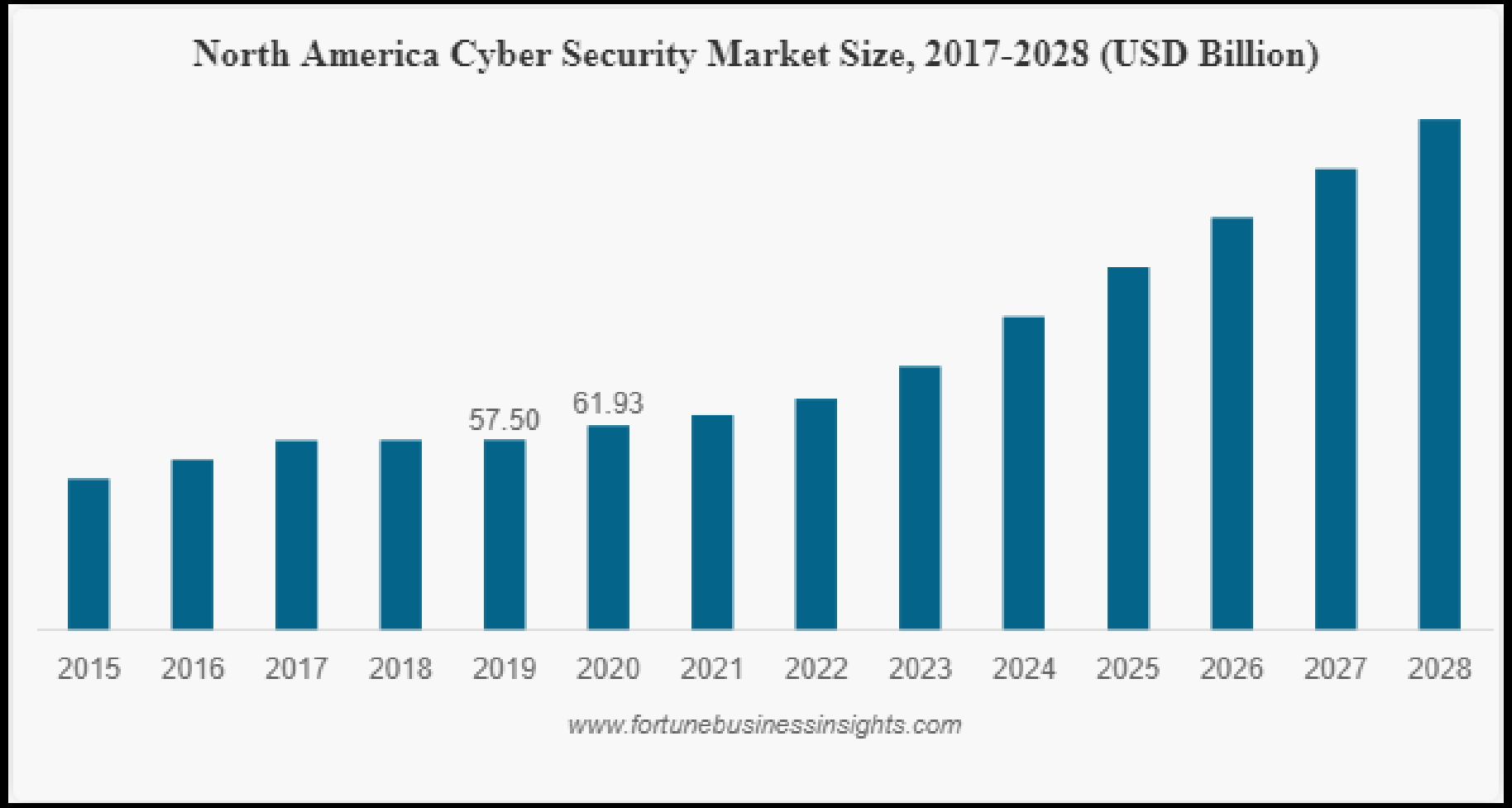
```
4141 4141 4141 4141 4141 4141 4141 4141 | AAAA AAAA AAAA AAAA
4141 4141 4141 4141 4141 4141 4141 4141 | AAAA AAAA AAAA AAAA
4141 4141 4141 4141 4141 4141 4141 4141 | AAAA AAAA AAAA AAAA
4141 4141 4141 4141 4141 4141 4141 4141 | AAAA AAAA AAAA AAAA
4141 4141 4141 4141 4141 4141 4141 4141 | AAAA AAAA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

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

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

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)

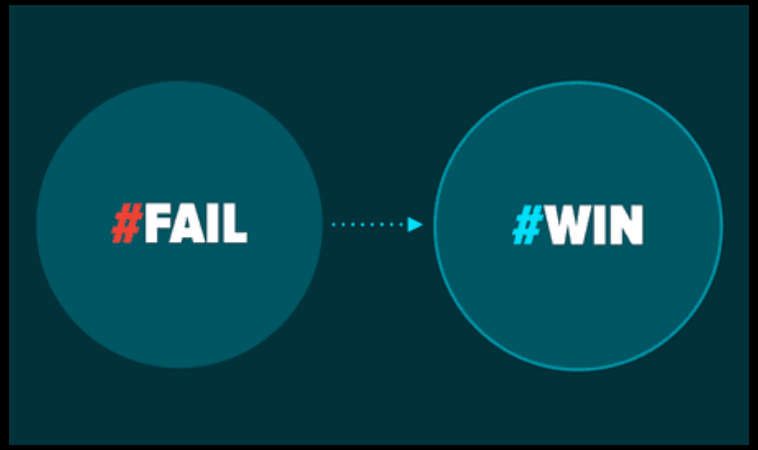
- Walk in during the day, stay until close
- Wait for someone to open a door, prop it open.
- Walk in with someone who is already authenticated
- Go up to the door and ask someone to let you in
- Find a door someone left open
- Pretend to be a delivery driver
- Get an authenticated card / key
- Wait 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

fakeScript

fakeScript - Syntax

Buffer = chunk of memory in your computer

makeBuffer(size)= creates a Buffer that is size **bytes** big

getInput(address) = gets **input** from the **user**, stores it at **address**

print(str) = standard print function

addressOf(Buffer buf) = returns where buf is inside the computer!

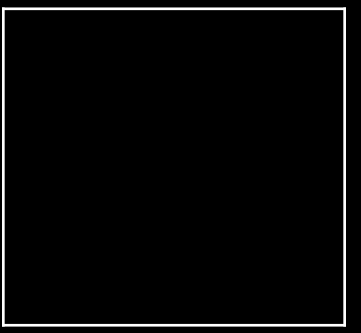
Standard conditionals apply

```
Example
if x
  then y
else
  z
```

fakeScript - Example code

```
01|  Buffer buf1 = makeBuffer(8)
02|  buf1 = “ABCDEFGH”
03|
04|  Buffer buf2 = makeBuffer(8)
05|  getInput(addressOf(buf2))
06|
07|  if buf1 == “ABCDEFGH”
08|    then print(“All operating normally”)
09|  else
10|    print(“ERROR: SYSTEM HACKED!”)
```

Output



```
>01|  Buffer buf1 = makeBuffer(8)
 02|  buf1 = "ABCDEFGH"
 03|
 04|  Buffer buf2 = makeBuffer(8)
 05|  getInput(addressOf(buf2))
 06|
 07|  if buf1 == "ABCDEFGH"
 08|    then print("All operating normally")
 09|  else
 10|    print("ERROR: SYSTEM HACKED!")
```

Memory

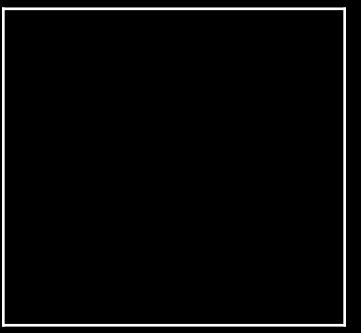
Output

```
 01|  Buffer buf1 = makeBuffer(8)
>02|  buf1 = "ABCDEFGH"
 03|
 04|  Buffer buf2 = makeBuffer(8)
 05|  getInput(addressOf(buf2))
 06|
 07|  if buf1 == "ABCDEFGH"
 08|    then print("All operating normally")
 09|  else
 10|    print("ERROR: SYSTEM HACKED!")
```

Memory

Memory is **added** from right to left but is **written** from left to right.

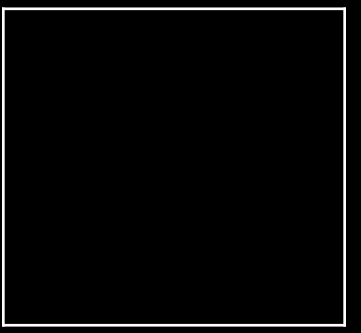
Output



```
 01|  Buffer buf1 = makeBuffer(8)
 02|  buf1 = "ABCDEFGH"
 03|
>04|  Buffer buf2 = makeBuffer(8)
 05|  getInput(addressOf(buf2))
 06|
 07|  if buf1 == "ABCDEFGH"
 08|    then print("All operating normally")
 09|  else
 10|    print("ERROR: SYSTEM HACKED!")
```

Memory

Output

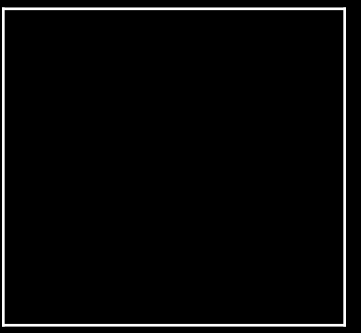


```
 01|  Buffer buf1 = makeBuffer(8)
 02|  buf1 = "ABCDEFGH"
 03|
>04|  Buffer buf2 = makeBuffer(8)
 05|  getInput(addressOf(buf2))
 06|
 07|  if buf1 == "ABCDEFGH"
 08|    then print("All operating normally")
 09|  else
 10|    print("ERROR: SYSTEM HACKED!")
```

Memory

BUF2	BUF2	BUF2	BUF2	BUF2	BUF2	BUF2	BUF2	A	B	C	D	E	F	G	H

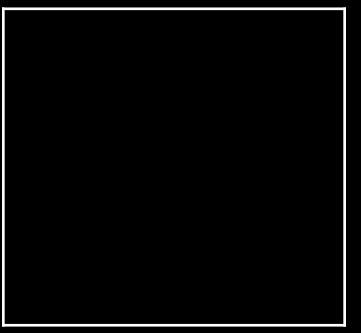
Output



```
 01|  Buffer buf1 = makeBuffer(8)
 02|  buf1 = "ABCDEFGH"
 03|
 04|  Buffer buf2 = makeBuffer(8)
>05|  getInput(addressOf(buf2))
 06|
 07|  if buf1 == "ABCDEFGH"
 08|    then print("All operating normally")
 09|  else
 10|    print("ERROR: SYSTEM HACKED!")
```

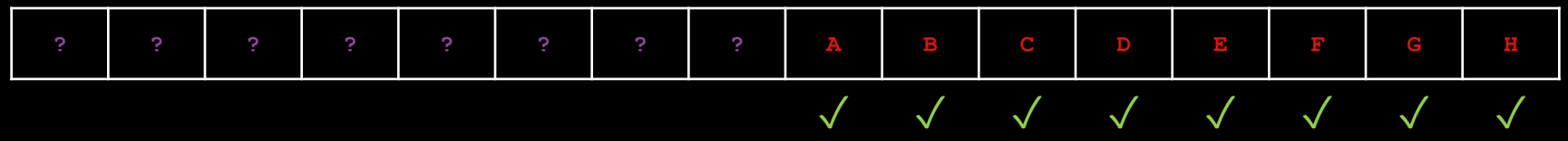
Memory

Output



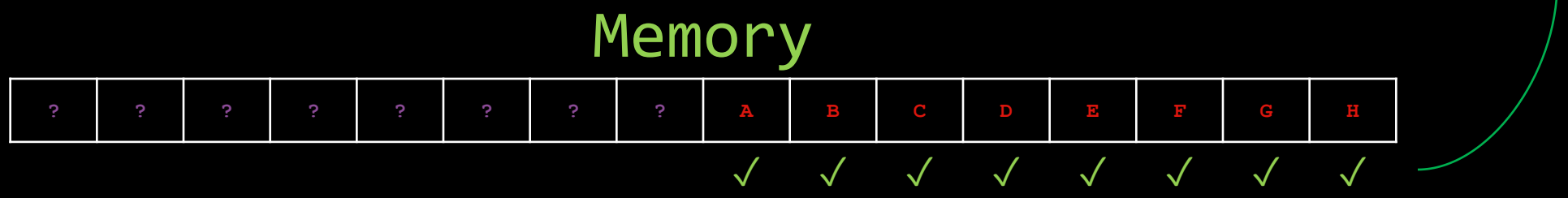
```
01|  Buffer buf1 = makeBuffer(8)
02|  buf1 = "ABCDEFGH"
03|
04|  Buffer buf2 = makeBuffer(8)
05|  getInput(addressOf(buf2))
06|
>07|  if buf1 == "ABCDEFGH"
08|    then print("All operating normally")
09|  else
10|    print("ERROR: SYSTEM HACKED!")
```

Memory



Output

```
 01|  Buffer buf1 = makeBuffer(8)
 02|  buf1 = "ABCDEFGH"
 03|
 04|  Buffer buf2 = makeBuffer(8)
 05|  getInput(addressOf(buf2))
 06|
>07|  if buf1 == "ABCDEFGH"
 08|    then print("All operating normally")
 09|  else
 10|    print("ERROR: SYSTEM HACKED!")
```



Output

```
"All operating
normally"
```

```
01|  Buffer buf1 = makeBuffer(8)
02|  buf1 = "ABCDEFGH"
03|
04|  Buffer buf2 = makeBuffer(8)
05|  getInput(addressOf(buf2))
06|
07|  if buf1 == "ABCDEFGH"
>08|    then print("All operating normally")
09|  else
10|    print("ERROR: SYSTEM HACKED!")
```

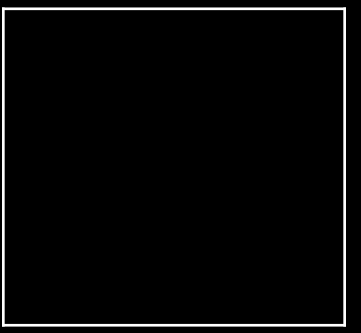
Memory

What assumptions were made?

Back to breakout rooms!

```
01|  Buffer buf1 = makeBuffer(8)
02|  buf1 = “ABCDEFGH”
03|
04|  Buffer buf2 = makeBuffer(8)
05|  getInput(addressOf(buf2))
06|
07|  if buf1 == “ABCDEFGH”
08|    then print(“All operating normally”)
09|  else
10|    print(“ERROR: SYSTEM HACKED!”)
```

Output



```
 01|  Buffer buf1 = makeBuffer(8)
 02|  buf1 = "ABCDEFGH"
 03|
>04|  Buffer buf2 = makeBuffer(8)
 05|  getInput(addressOf(buf2))
 06|
 07|  if buf1 == "ABCDEFGH"
 08|    then print("All operating normally")
 09|  else
 10|    print("ERROR: SYSTEM HACKED!")
```

Memory

?	?	?	?	?	?	?	?	A	B	C	D	E	F	G	H

Output

```
 01|  Buffer buf1 = makeBuffer(8)
 02|  buf1 = "ABCDEFGH"
 03|
 04|  Buffer buf2 = makeBuffer(8)
>05|  getInput(addressOf(buf2))     <<< Size Check ?
 06|
 07|  if buf1 == "ABCDEFGH"
 08|    then print("All operating normally")
 09|  else
 10|    print("ERROR: SYSTEM HACKED!")
```

Memory

Output

```
01|  Buffer buf1 = makeBuffer(8)
02|  buf1 = "ABCDEFGH"
03|
04|  Buffer buf2 = makeBuffer(8)
05|  getInput(addressOf(buf2))      <<< Size Check ?
06|
>07|  if buf1 == "ABCDEFGH"
08|    then print("All operating normally")
09|  else
10|    print("ERROR: SYSTEM HACKED!")
```

Memory

?	?	?	?	?	?	?	?	?	?	?	D	E	F	G	H
✓	✓	✓	✓	✓	✓	✓	✓	X	X	X					

Output

```
ERROR: SYSTEM
HACKED!
```

```
 01|  Buffer buf1 = makeBuffer(8)
 02|  buf1 = "ABCDEFGH"
 03|
 04|  Buffer buf2 = makeBuffer(8)
 05|  getInput(addressOf(buf2))      <<< Size Check ?
 06|
 07|  if buf1 == "ABCDEFGH"
 08|    then print("All operating normally")
 09|  else
>10|    print("ERROR: SYSTEM HACKED!")
```

Memory

What was that?

- Buffer overflow attack!
- Memory safe vs unsafe programming languages
- Can be used to do really cool stuff

How can we defend against that attack?

Output

```
ERROR: SYSTEM
HACKED!
```

```
01|  Buffer buf1 = makeBuffer(8)
02|  buf1 = "ABCDEFGH"
03|
04|  Buffer buf2 = makeBuffer(8)
05|  getInput(addressOf(buf2),8)  << Add A Size!
06|
07|  if buf1 == "ABCDEFGH"
08|    then print("All operating normally")
09|  else
10|    print("ERROR: SYSTEM HACKED!")
```

Memory

Questions?

Learning Security

Learning Security is Hard

- Not many resources for newcomers
  - Resources have higher barrier to entry

Solution

- “Gameify” the hell out of it
  - Turn learning into a game

CTF

- Capture the Flag
  - picoctf, UIUCTF!!!

An IRL CTF before the Pandemic at The Disco

CTF – Helpful Resources

Get started with CTFs! Here are some great ones to try out!

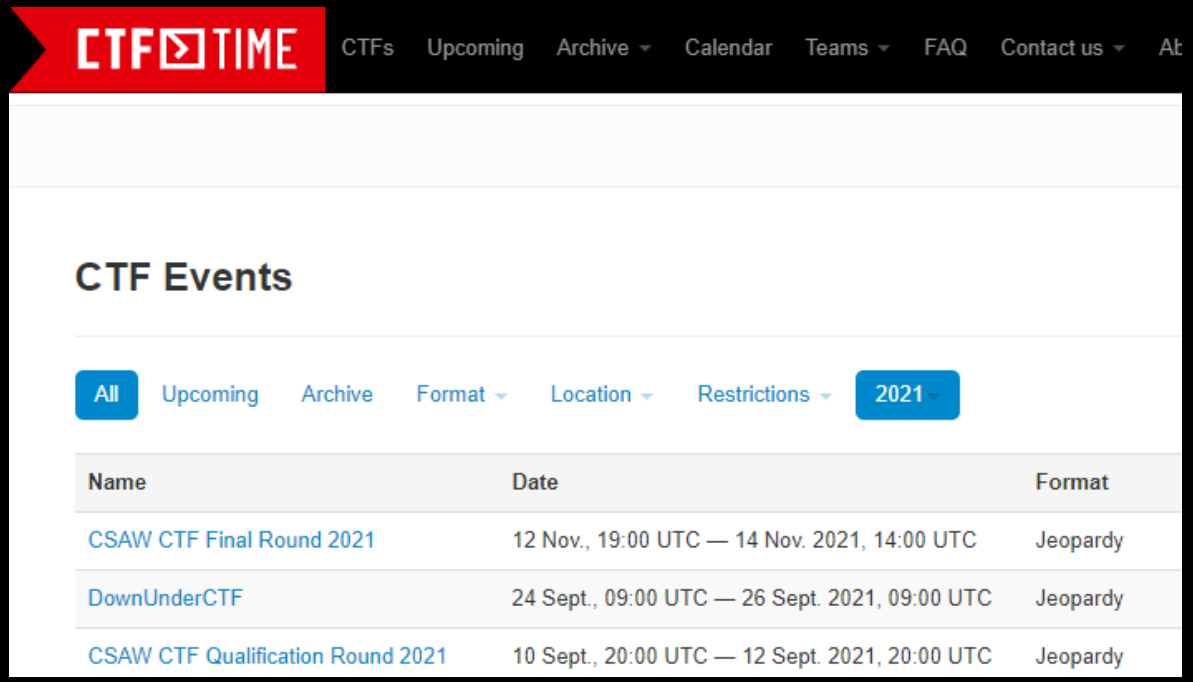
bandit (overthewire, do through 15-20) << Start Here!

natas (overthewire, do through 10)

picoctf (https://picoctf.org/competitions/past.html)

UIUCTF, SIGPwny year-round CTF

hackthebox << more advanced!



Core Security Topics (As Seen @CTFs)

- RE / PWN
- Web
- Crypto
- “Misc”

RE / PWN

- What many people think about when they think about traditional hacking
- Attacking systems, elevating access, pwning things
- fakeScript was a pwn challenge

Term List
Buffer Overflow, Stack Smashing, Heap Attacks, Ret-To-Libc, Return Oriented Programming (ROP), Global Offset Table (GOT), Dynamic Linker Injection, Privilege Escalation

This list could go on forever

```
struct group_info init_groups = { .usage = ATOMIC_INIT(2) };
struct group_info *groups_alloc(int gidsetsize){
    struct group_info *group_info;
    int nblocks;
    int i;

    nblocks = (gidsetsize + NGROUPS_PER_BLOCK - 1) / NGROUPS_PER_BLOCK;
    /* Make sure we always allocate at least one indirect block pointer */
    nblocks = nblocks ? : 1;
    group_info = kmalloc(sizeof(*group_info)
```

Web

- Attacking websites and web infrastructures
- Analyzing and finding vulnerabilities in the modern internet
- Check out https://overthewire.org/wargames/natas/ if you want to start doing web hacking

Term List
SQL Injections, Inspect Element, CSRF (Cross Site Request Forgery), XSS (Cross Site Scripting), Replay Attacks, Cookie Injection, Flash Attacks, DNS Spoofing

This list could also go on forever…

Cryptography

- Attack the cryptographic structures that allow for secure communication
- CIA Model (Confidentiality, Integrity, Availability)
- Break Crypto -> Break the World

Term List
AES, RSA, Padding Oracles, KPA/KCA, Partial/Full Homomorphism, Public and Private Key Encryption, Blockchain, Hashing, MD5, Sha256

This list could ALSO go on forever…

“Misc”

- Forensics
  - Finding digital information about systems, utilizing and analyzing that information
- OSINT
  - Utilizing public and semi-public information to gather information about targets
- Networking
  - Analyzing and attacking the actual communication process between hosts
- Kernel
  - Attacking the foundational software that operating systems run on
- Human Security
  - Attacking the weakest link in the chain: humans (this often works wonders)

This list also goes on forever…

For real… Forever!

Social Engineering

Physical Security

Opsec

System Security

Steganograpy

Hardware Security

Social Media Attacks

Health Security

IT Security

Educational Security

Institutional Security

Phishing and Spear Phishing

Wi-Fi Security

Corporate Security

Humanitarian Security

Government Security

Questions?

Cybersecurity is huge!

So where can you end up?

Career Paths

Cybersecurity Career Paths

- Researcher
  - Educational, Corporate, Government
- Security Software Team
  - MalwareBytes (UIUC Alum!)
  - Google Security (Parisa Tabriz!)
- Security Tool Development
  - IDA, Maltego
- Pentester
  - Consultant, Corporate
- SOC Analyist
  - Monitor and defend networks
- Cyber Forensics
  - OSINT and Forensics as a profession
- Threat Intelligence
  - Monitoring disinformation campaigns
- Security Law
  - We need competent people
- Professor
  - Educate the future!
- Security Influencer
  - Talk trash on Twitter with Tay!

Questions?

Security Opportunities at UIUC

There are lots!

Security Opportunities At UIUC

- CS461, CS463, CS563, CS498-Applied Crypto, CS498-AI Security, CS598 – OS Security, Secure Processor Design
  - More classes coming soon!
- Research
  - We are an awesome research university
- SIGPwny
  - More info at https://sigpwny.com/
  - Reach out to me
- ICSSP
  - Get paid to go to school!
  - Work for the government

Questions?

About security, security opportunities, UIUC etc.

References

1. https://www.securityroundtable.org/cybersecurity-adversary-mindset/