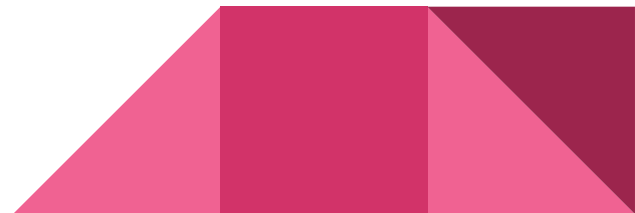


Cyber@UC Meeting 51

Reverse Engineering: Android apps and more

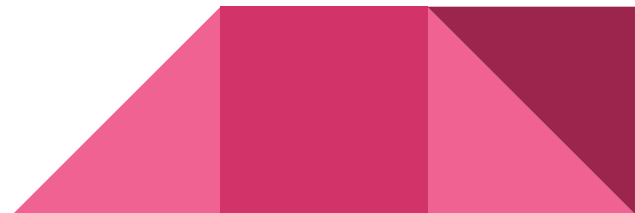
If You're New!

- Join our Slack: ucyber.slack.com
- **SIGN IN!** (*Slackbot will post the link in #general*)
- Feel free to get involved with one of our committees:
Content Finance Public Affairs Outreach Recruitment
- Ongoing Projects:
 - Malware Sandboxing Lab
 - Cyber Range
 - RAPIDS Cyber Op Center



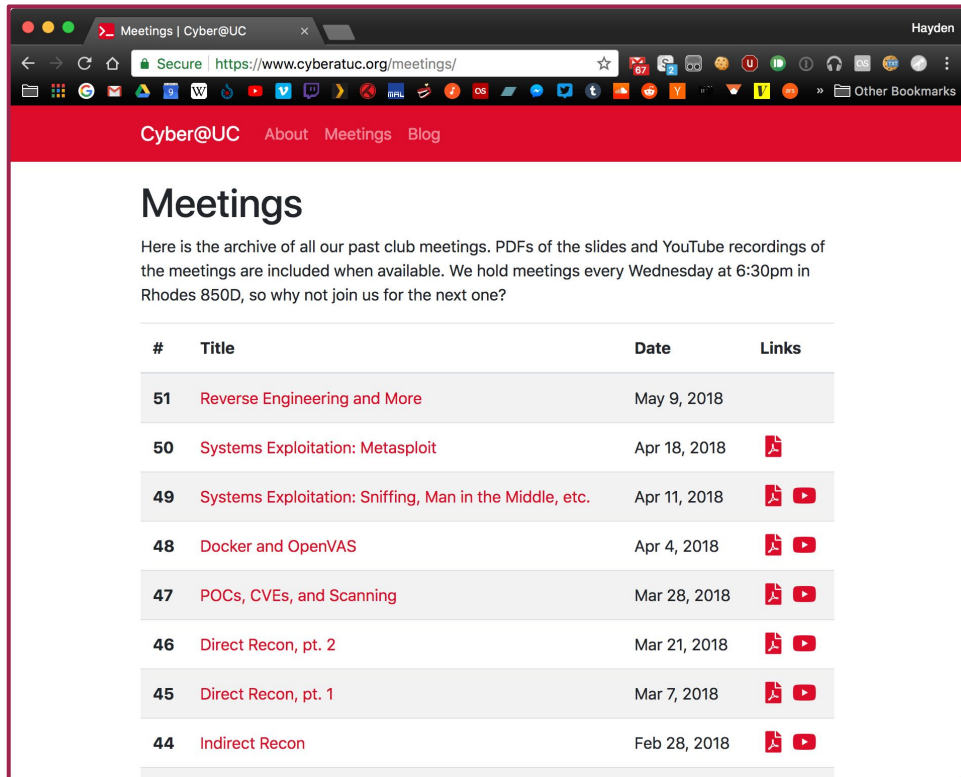
Announcements

- **Welcome back!**
- BSides Cincy THIS SATURDAY bsidescincy.org
- We got access to ERC 516!
 - ...but the server racks are the wrong size >.<
 - Also waiting on switches, tables, desktop PCs, etc
- **ThinkCyber Fellowship** July 13–16 think-cyber.com
- Partnership with **Galois** in the works



New website

- Soft launched! [cyberatuc.org](https://www.cyberatuc.org)
- Archive of old meetings now up
- Everyone can contribute:
github.com/UCyber/cyberatuc.org
- Feedback and contributions welcomed! (pleeeeeease)
















Meetings | Cyber@UC

Secure | <https://www.cyberatuc.org/meetings/>

Cyber@UC About Meetings Blog

Meetings

Here is the archive of all our past club meetings. PDFs of the slides and YouTube recordings of the meetings are included when available. We hold meetings every Wednesday at 6:30pm in Rhodes 850D, so why not join us for the next one?

#	Title	Date	Links
51	Reverse Engineering and More	May 9, 2018	
50	Systems Exploitation: Metasploit	Apr 18, 2018	
49	Systems Exploitation: Sniffing, Man in the Middle, etc.	Apr 11, 2018	 
48	Docker and OpenVAS	Apr 4, 2018	 
47	POCs, CVEs, and Scanning	Mar 28, 2018	 
46	Direct Recon, pt. 2	Mar 21, 2018	 
45	Direct Recon, pt. 1	Mar 7, 2018	 
44	Indirect Recon	Feb 28, 2018	 

Public Affairs

Useful videos and weekly livestreams on **YouTube**:

youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us for club updates and cybersecurity news:

- **Twitter:** [@CyberAtUC](https://twitter.com/CyberAtUC)
- **Facebook:** [@CyberAtUC](https://facebook.com/CyberAtUC)
- **Instagram:** [@CyberAtUC](https://instagram.com/CyberAtUC)

For more info: ucyber.github.io or cyberatuc.org



Weekly Content

NSA exabyte data center

- "Intelligence Community Comprehensive National Cybersecurity Initiative Data Center"
- 100,000 sq. ft. of data center space in Utah
- Capacity: 3–12 exabytes
 - Probably just 3 EB
- 3 EB \approx 949 billion copies of Aqua's "Barbie Girl"
 - 5 EB \approx all words ever spoken by human beings
- Cost: \sim \$1.5 billion
- Why Utah?
 - Room to expand
 - Low utility rates
 - Low potential for natural disasters
 - Easy access to water for cooling



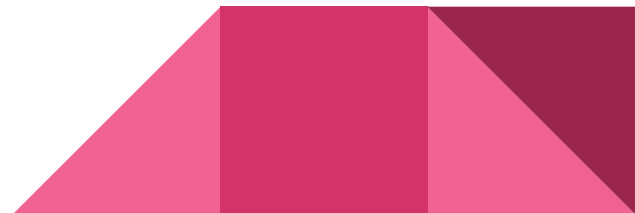
Sources for NSA data center

https://en.wikipedia.org/wiki/Utah_Data_Center

<https://www.zmescience.com/science/how-big-data-can-get/>

<https://www.theblaze.com/news/2013/07/01/seven-stats-to-know-about-nsas-utah-data-center-as-it-nears-completion>

<https://techcrunch.com/2013/07/24/the-nsas-massive-utah-data-center-wont-store-anything-close-to-yottabytes-of-data/>



NSA phone record surveillance

- NSA collected 534 million call records last year
 - Triple what it collected in 2016
- Not expected to be indicative of a trend, but a number that fluctuates
- 129,080 individuals subjected to warrantless spying, 20% increase
 - 45% in the last five years

<https://www.reuters.com/article/us-usa-cyber-surveillance/spy-agency-nsa-triples-collection-of-u-s-phone-records-official-report-idUSKBN1I52FR>

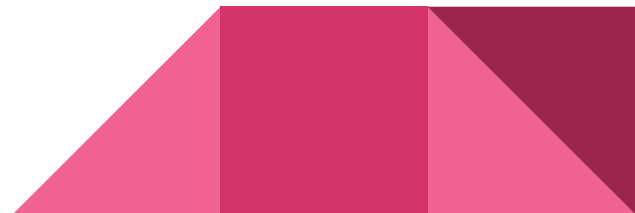
<https://www.cnn.com/2013/06/05/politics/nsa-verizon-records/>



Twitter end-to-end encrypted messaging

- Currently in small-scale testing
- Following example of WhatsApp, iMessage, Facebook Messenger, etc
- Not enabled by default
 - Facebook Messenger encryption works this way too
- No infrastructure for secure storage of keys

<https://thehackernews.com/2018/05/encrypted-twitter-direct-messages.html>





gnireenignE esreveR

(get it? get it?)

What is gnireenignE esreveR?

It's Reverse Engineering spelled in reverse

(Chris thinks he's really funny for adding this slide)



What is Reverse Engineering?

Generally:

- Applying the scientific model to a man-made object rather than a natural phenomenon

In Cyber:

- Analyzing systems to figure out their insides without always knowing their exact contents (black box)



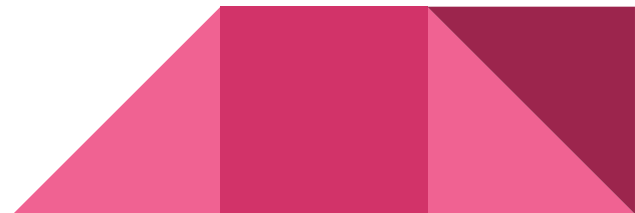
Reverse Engineering in the News

- Malware Analysis
- Remote Server Exploitation
 - APIs of all sorts
 - Games
- Protocol Spoofing
 - Iran–U.S. RQ-170 incident (Used GPS/GNSS Spoofing)



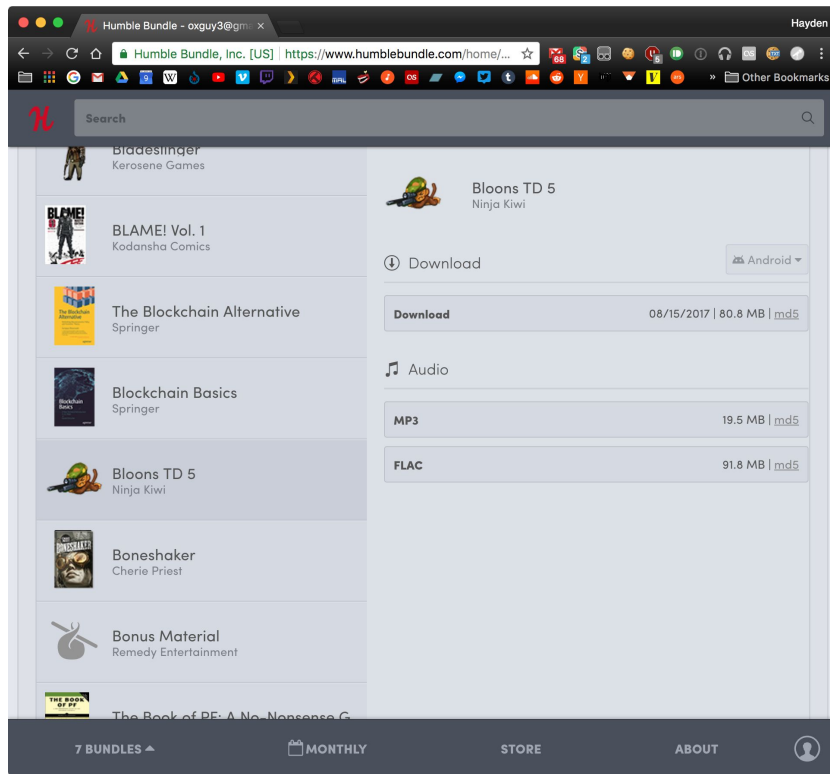
Common RE Tools

- Disassemblers
 - IDA
 - OllyDbg
- Packet/traffic inspection tools
 - Wireshark
 - mitmproxy, Fiddler, Charles
- Memory inspectors / editors
 - Cheat Engine
- Process monitors



Our target: Humble Bundle

- I want to automate downloading my vidya games
- No API... scrape the website?
 - But scraping suuuucks
- Oh, they have an Android app!



Decompiling the app

- APK download: humblebundle.com/app
 - (for Play Store apps, use this to get an APK: apps.evozi.com/apk-downloader)
- How can we open it?
- Apktool!



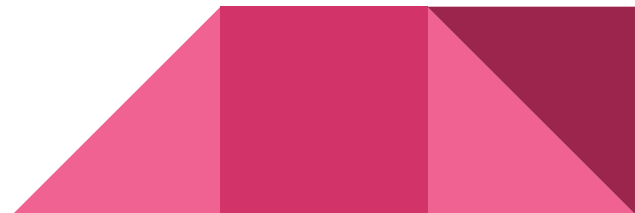
Apktool

- Installation

- Kali/Ubuntu/Debian: **sudo apt-get install apktool**
- macOS: **brew install apktool**
- Everyone else: ibotpeaches.github.io/Apktool/install/

- Basic usage

- Decompile an app: **apktool d MyApp.apk**
- ...that's it!



<demo>

What is Smali?

- Low-level, esqre language
- Basically a text version of Java bytecode
- It's awful, but we don't have to master it
 - Just need to be able to sorta-kind read it



Java vs. Smali

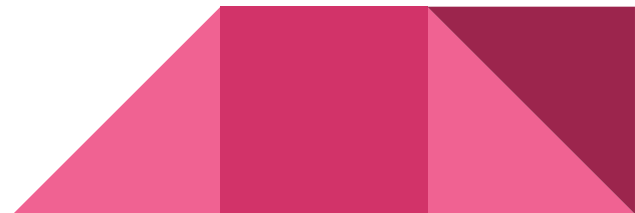
```
public class HelloWorld {  
    public static void main(String[] args) {  
        System.out.println("Hello World!");  
    }  
}
```

```
.class public LHelloWorld;  
  
.super Ljava/lang/Object;  
  
.method public static main([Ljava/lang/String;)V  
    .registers 2  
  
    sget-object v0,  
Ljava/lang/System;->out:Ljava/io/PrintStream;  
  
    const-string v1, "Hello World!"  
  
    invoke-virtual {v0, v1},  
Ljava/io/PrintStream;->println(Ljava/lang/String;)V  
  
    return-void  
.end method
```

<demo>

Postman

- GUI tool for testing APIs and making HTTP requests
- Much easier than memorizing `curl` flags
- Download: getpostman.com



<demo>

Other approaches/tools

- Intercepting HTTP traffic
 - Web debugging proxies: **mitmproxy** (universal), **Fiddler** (Windows), **Charles** (macOS)
 - Mini demo: [Wepa Print App](#)
- For web apps: your browser's developer tools
 - Mini demo: [USL players](#)

