

# Cyber@UC Meeting 67

Bash and OverTheWire

# If You're New!

- Join our Slack: [cyberatuc.slack.com](https://cyberatuc.slack.com) (URL changed!)
- **SIGN IN!** (*Slackbot will post the link in #general every Wed@6:30*)
- Feel free to get involved with one of our committees:  
*Content Finance Public Affairs Outreach Recruitment*
- Ongoing Projects:
  - Research lab!



# Announcements

- Board game night went great!
- **September 18th** NSA visit with an **Enigma Machine**
  - Deli Food!
- **US Bank visit** date!
- **Rockwell Security Seminar**
  - September 20th 9am-3pm
  - Nippert Stadium
- Lab update: [SOC Architecture](#)



# Public Affairs

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

[youtube.com/channel/UCWcJuk7A\\_1nDj4m-cHWvIFw](https://youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw)

Follow us for club updates and cybersecurity news:

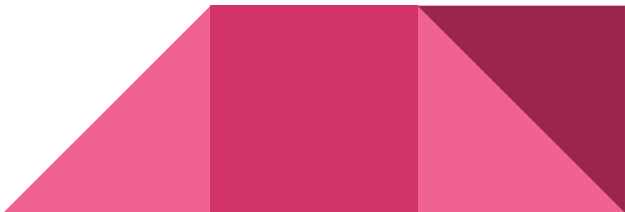
- **Twitter:** [@CyberAtUC](https://twitter.com/CyberAtUC)
- **Facebook:** [@CyberAtUC](https://facebook.com/CyberAtUC)
- **Instagram:** [@CyberAtUC](https://instagram.com/CyberAtUC)

For more info: [cyberatuc.org](https://cyberatuc.org)



# Weekly Content

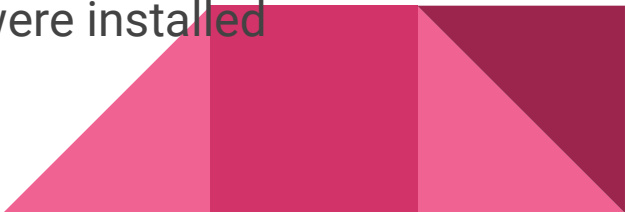
# Windows ALPC Zero-Day

- Disclosed last week and confirmed to work on fully patched Windows 10 systems, also included a PoC
  - Vulnerability allows for privilege escalation of a local user or malicious program
  - Advanced Local Procedure Call (ALPC) is an internal mechanism of the Windows OS that facilitates fast and secure data transfer between processes
  - Can even allow escalation to SYSTEM level privileges
  - ALPC interface is a local system reducing impact of the vulnerability
  - Microsoft was not notified of the zero-day
  - Patch is unlikely to be released until September 11
- 

# Fortnite for Android MitD

- Epic Games made the decision not to make 'Fortnite for Android' available through the Google Play Store, but through their own app instead
- Installing Fortnite will require the installation of a helper app which will download fortnite to the phone's storage and install it
- Any app with "WRITE\_EXTERNAL\_STORAGE" permissions could intercept the installation and replace the file with a different malicious APK
- The malicious app could have full permissions, including access to SMS, GPS, camera, etc. without user knowledge
- Vuln found and reported August 15th, patched withing 48 hours v 2.1.0
- Epic Games CEO criticized researcher for disclosing vuln within 7 days

# Triout Android Spyware Framework

- Corrupts legitimate apps into spyware
  - Capable of recording calls, monitoring texts, stealing photos/videos, collecting location data, hides itself
  - First spotted by Bitdefender May 15th, someone in Russia uploaded it to VirusTotal
  - App maintained the same look and capabilities of the original
  - Malware does not currently use obfuscation, allowing researchers to obtain source code
  - Not yet sure how the malicious versions of the app were installed
- 



# Recommended Reading

<https://thehackernews.com/2018/08/google-titan-security-key.html>

<https://www.welivesecurity.com/2018/09/03/majority-worlds-top-websites-https/>

<https://thehackernews.com/2018/08/reality-winner-nsa-russia.html>

<https://krebsonsecurity.com/2018/08/experts-urge-rapid-patching-of-struts-bug/>



# Recommended Reading (breaches)

<https://thehackernews.com/2018/08/t-mobile-hack-breach.html>

<https://thehackernews.com/2018/08/air-canada-data-breach.html>

<https://krebsonsecurity.com/2018/08/fiserv-flaw-exposed-customer-data-at-hundreds-of-banks/>

<https://thehackernews.com/2018/09/google-mastercard-advertising.html>

<https://thehackernews.com/2018/08/facebook-vpn-app-apple-store.html>

<https://krebsonsecurity.com/2018/08/instagrams-new-security-tools-are-a-welcome-step-but-not-enough>

<https://thehackernews.com/2018/08/secure-instagram-account.html>





# Bash

# What is Bash?

- 
- Command Line Interpreter (CLI)
- Most popular shell on Linux
- Features
  - Runs programs
  - Stores Variables
  - Piping
  - Conditional Logic

```
#!/bin/bash
```



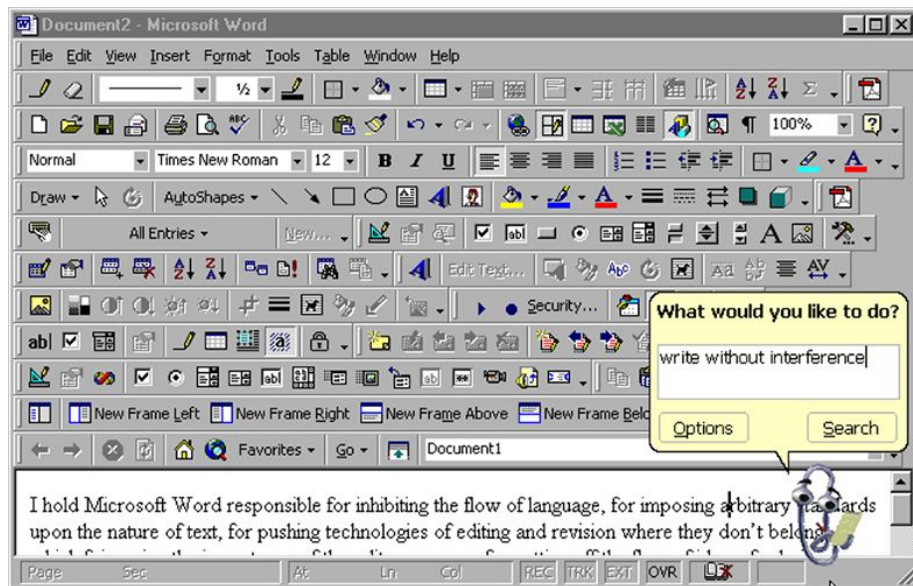
# GNU / Linux

- Bash wouldn't have much use without programs
- GNU ported Unix tools to Linux.
- Some of the popular tools
  - ls
  - cd
  - mv
  - pwd
  - cat
  - less



# Why use Bash?

- Complex tools use CLI
- You have better control over the software
- CLI is very powerful in the hands of the experienced
- Tab autocomplete actually works



# SSH

- Secure Shell
- Used for secure remote connection to other machines.
- Replaces Telnet/RSH as a secure alternative
- Present login and show a Bash terminal
- Technologies built on top of or extended by SSH
  - SFTP (SSH File Transfer Protocol)
  - SCP (CP over SSH)
  - SOCKS protocol (Proxying)
  - X11 Forwarding (Super Magical)
  - Reverse / Local Port Binding (Magical)



# Connecting to overthewire.org

overthewire.org – suggested starting game is *Bandit*

Hostname: `bandit.labs.overthewire.org` (on port 2220)

Username: `bandit0`

Password: `bandit0`

Bash command:

```
ssh bandit0@bandit.labs.overthewire.org -p2220
```

