

# Cyber@UC Meeting 35

Exploit ALL the vulnerabilities!

# If You're New!

- Join our Slack **ucyber.slack.com**
- Follow us on **Twitter @UCyb3r** and Facebook UC.yber; University of Cincinnati OWASP Chapter
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment**
- Stay updated through our weekly emails and SLACK



# Announcements

- **Red team** against Franco's Class! *TOMORROW*
- **P&G visit set for Jan 22nd 2-3pm**
- **Logo Design** SUBMIT IDEAS!
- We have **200K of equipment** coming!
- **Lab in ERC almost ready** getting keys soon!



# Weekly Content


# Cybersec staffing problems causing vulnerability

- 22% of surveyed companies cited their security team as being understaffed
- The skills shortage expected to create 1.8 million job deficit by 2022
- Constant advancement in the field makes maintaining skills difficult
- We are seeing that the deficit is a skills deficit, less a worker deficit
- It is difficult to attain the necessary skills while currently working in the field due to the heavy workload
- 88% of security professional respondents report moderate to high job satisfaction
- Incentives such as financial and other forms of compensation are reported as the reason for this high level of satisfaction

# Immunity for AV Vendors

- Malwarebytes was sued for listing Enigma Software Group tools as malware because they filed a lawsuit against their affiliate Bleepingcomputer.com
- Malwarebytes made use of a poorly known provision in the Communications Decency Act
- “provides legal immunity to computer vendors that provide “technical means to restrict access” to obscene, lewd, excessively violent, and otherwise objectionable content”
- Vendors are able to self define what they view as objectionable content

<https://www.darkreading.com/cloud/av-vendors-have-immunity-for-malware-blocking-decisions-court-says/d/d-id/1330385?>





# Exploit Breakout Sessions

# Overview of Targets

## Services to Target:

- FTP (File Transfer Protocol)
- IPP (Printer Service)
- Ping
- Daytime
- MySQL
- WordPress
- Apache2
- PHP





# Vulnerabilities

- Changes in the configuration files
  - ~/.bashrc added aliases for “sudo” and updated to make sure that they **don't** get root access
- CVE-2015-5477 BIND9 TKEY remote assert DoS PoC
  - Tkill.c file included in the OS and added as a startup application
- Shell script[4][5] to stop running services
  - A script that stops local services
- Dirty Cow
  - Gives root access without prompting the attacker for to enter the password



# Additional Info

- Targeted services will be monitored
  - Points will be deducted if they go down
- Login will be done Via OpenVPN
  - Franco will provide the keys



# Team Goals

Map out a plan for exploiting  
and taking down services

- Pick a Service
  - Choose method of recon
  - Choose Vulnerability
  - *Research*, **RESEARCH**  
RESEARCH
  - Test out the commands
  - Write that BASH!
-