Cyber@UC Meeting 36

Red Team Recap

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

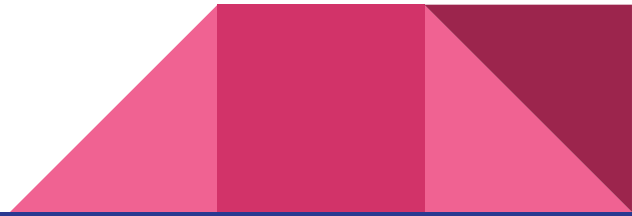
- **Red team** against Franco's Class! *TOMORROW*
- **P&G visit set for Jan 22nd 2-3pm**
- **Logo Design** SUBMIT IDEAS!
- We have **200K of equipment** coming!
- **Lab in ERC almost ready** getting keys soon!

Weekly Content

MailSploit (Email spoofing)

- Collection of over 33 popular email client were vulnerable
  - 8 have patched already and 12 more are implementing a fix currently
- Problem arises from a lack of input sanitization by email clients
- Using a combination of control characters, like newline, the domain portion of an email can be hidden

https://thehackernews.com/2017/12/email-spoofing-client.html



Jail hacker going to jail

- A 27-year-old Michigan man now faces prison time
- He hacked into the jail's network to try and get a friend released early
- Called prison staff, claiming to be the jail's IT department, and tricked them into downloading and running malware by visiting a malicious website
- Using newly obtained remote login information, he installed malware on the County's network to access their sensitive XJail system
- On top of stealing thousands of sensitive files and documents, he also altered 1 prisoner's records for early release
- Jail employees detected changes and brought in the FBI
- Estimated costs for the incident are $235,000

https://thehackernews.com/2017/12/hacking-jail-records.

Bitcoin sites are a new DDoS focus

- The massive surge in Bitcoin prices has brought renewed attention to the currency and its exchanges
- They have been a recent target for many DDoS attacks
  - Ex. The bitcoin-us currency exchange Bitfinex
- Nearly 3 of every 4 Bitcoin sites that uses Imperva's services were hit with DDoS attacks in the last quarter
- Ranked up to one of the top 10 most DDoS'd services in 2017 quarter 3
- Believe that criminals are attempting to develop profit from price/speculation fluctuations

https://www.darkreading.com/vulnerabilities---threats/bitcoin[illegible]-become-[illegible]a
rgets-for-ddos-attacks/d/d-id/1330556

Exploit Breakout Sessions

Overview of Targets

Services to Target:

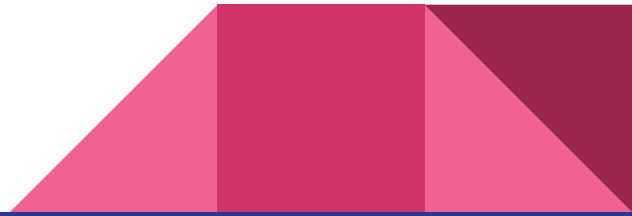
- FTP (File Transfer Protocol)
- IPP (Printer Service)
- Ping
- Daytime
- MySQL
- WordPress
- Apache2
- PHP

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

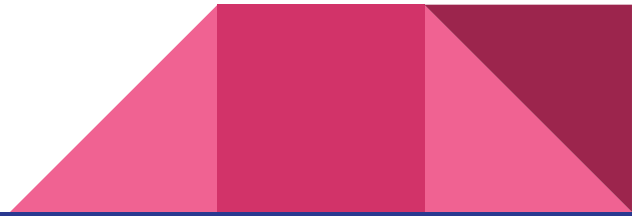
Tools!

- OpenVas
- nmap
- Metasploit
- Searchsploit
- Armiatge
- Cobalt Strike



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!