Cyber@UC Meeting 64

Wireless Auditing and Monitoring Tools

If You’re New!

- Join our Slack: **ucyber.slack.com**
- **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:
  - RAPIDS Lab!

Lab updates

- We have **desks**!!
- Next steps
  - Running ethernet/making cables
  - Creating standard Debian image
  - Setting up servers with OpenStack+etc

Other announcements

- **September 18th** NSA visit with an **Enigma Machine**
  - We need to decide on the **food we want**
- **US Bank visit** in the works
- Visiting **Stebbins High School** early fall!
- **NSA Scholarship** Opportunities!
- CiNPA Security Meetup **Tomorrow**!
  - Physical Security Night
  - 225 Pictoria Drive, Springdale, Ohio 45246
  - 6:30pm

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
- **Facebook:** @CyberAtUC
- **Instagram:** @CyberAtUC

For more info: cyberatuc.org

Weekly Content

Faxploit

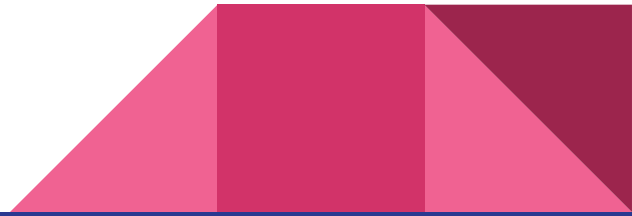
- Using vulnerabilities in fax machines, an attacker can compromise your network by sending a specially crafted image file
- Most fax machines are part of all-in-one printers that are connected to the company's network
- Using two buffer overflows, parsing COM markers and then DHT markers
  - Allows remote code execution
- Firmware patches are available for HP, other fax-based printers could also be vulnerable

https://thehackernews.com/2018/08/hack-printer-fax-machine.html

Man-in-the-Disk

- Exploits how Android apps use ‘External Storage’ to store app data that is vulnerable to code injection
- Monitoring the request for data from external storage, data can be intercepted and modified

https://thehackernews.com/2018/08/man-in-the-disk-android-hack.html



Cashout Blitz

- FBI warning banks that cybercriminals plan to carry out a highly choreographed, global fraud scheme known as an “ATM cashout”
- FBI obtained reporting indicating this would occur, believed to come from a card issuer being breached
- Perpetrators are also expected to use exploits to allow them to alter account balances and withdraw an unlimited amount of money

https://krebsonsecurity.com/2018/08/fbi-warns-of-unlimited-atm-cashout-blitz/

Recommended Reading

https://thehackernews.com/2018/08/artificial-intelligence-malware.html

https://securelist.com/keypass-ransomware/87412/

https://www.welivesecurity.com/2018/08/13/cramming-code-bugs-secure/

https://securelist.com/apt-trends-report-q2-2018/86487/

https://thehackernews.com/2018/08/google-mobile-location-tracking.html

https://thehackernews.com/2018/08/macos-mouse-click-hack.html

Recommended Reading (continued)

https://thehackernews.com/2018/08/android-app-hack.html

https://thehackernews.com/2018/08/android-app-hack.html

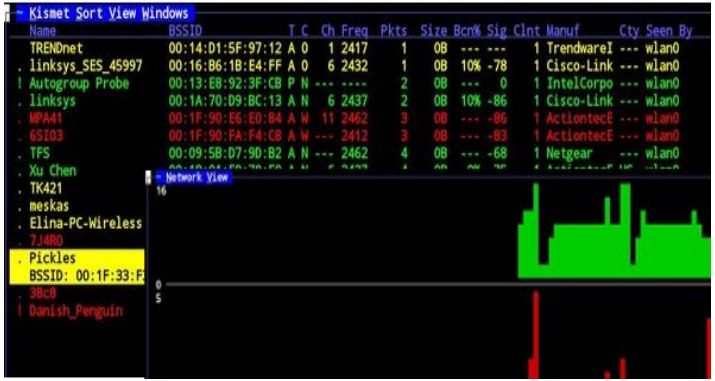
https://www.darkreading.com/risk/flaws-in-mobile-point-of-sale-readers-displayed-at-black-hat/d/d-id/1332555

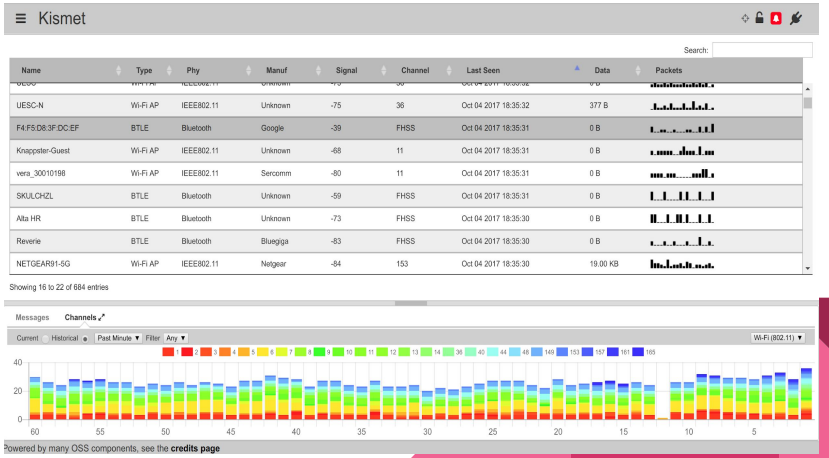
https://www.uc.edu/hr/ssc/training-resources/online-with-lynda.html (Free Lynda Account through UC)

Wireless auditing & monitoring tools

Kismet

- Customizable wireless intrusion detection tool
- Multiple interface options, can run as a service





Airgeddon

- Easy-to-use wireless auditing script for linux
- Uses of lots of different tools together (aircrack-ng suite, BeEF, ettercap, ect.)
- Supports Evil twin attacks
- Functions similarly to the social engineering toolkit (SET)

Wifite

- Wireless auditing tool meant to make audits very easy
- Attacks WEP, WPA, and WPA2
- Very noticeable, stealth is not prioritized

To install you can go to the GitHub page: https://github.com/derv82/wifite2 or

```
git clone https://github.com/derv82/wifite2.git
cd wifite2
python Wifite.py
```