Cyber@UC Meeting 55

Wireshark Demo

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

- Lots of updates to **our website**
  - First blog post—regular posts planned [cyberatuc.org/blog]
  - Spiffy new about page with headshots [cyberatuc.org/about]
  - Want to contribute? [cyberatuc.org/guides/website]
- We got a new **server rack** in!
- **Towson University** Cyber Club Partnership
- **CAECO** NSA funding opportunity to design a cyber operations competition

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

Sound based hard drive attack

- Remember when speakers were used to send data out of secured computer?
- Using acoustic resonance, a computer's own speakers can be used to cause a false positive to be read in the HDDs shock sensor
- False positives cause the drive to unnecessarily park its head
- Demonstrated its use against cctv systems and desktop computers
- Attack can be done from any nearby speaker or by attaching a malicious sound file to an email or web page
- The stopping of the head can be used to crash the device
- The team that found this has proposed a possible firmware update for a new controller

ZipSlip

- British software firm snyk found a vuln affecting thousands of projects that can allow code execution of targeted systems
- The vulnerability is an arbitrary file overwrite vuln that triggers directory traversal attack while extracting files from an archive and affects many formats such as:
  - Tar, jar, war, cpio, apk, rar, and 7z
- 1000s of projects in many languages have vulnerable libraries, incl. OWASP
- Exploited through a special archive containing directory traversal filenames
- Can even overwrite legitimate files

Drupalgeddon2, why haven’t you patched?

- Drupalgeddon2 is a critical RCE vuln discovered in late March that could allow an attacker to take over vulnerable sites
- It allows unauthed remote attackers to execute malicious code on default or standard Drupal installations
- Despite patches being released, over 115,000 vulnerable sites have been found by security researcher Troy Mursch, who scanned “the whole internet”
- Drupalgeddon2 is currently being used to inject cryptominers
- Some sites have made the upgrade, but were already infected and have not yet removed the malicious code

Recommended Reading

- https://thehackernews.com/2018/06/microsoft-acquires-github.html
- https://thehackernews.com/2018/06/apple-macos-mojave.html
- https://krebsonsecurity.com/2018/06/researcher-finds-credentials-for-92-million-users-of-dna-testing-firm-myheritage/
- https://www.darkreading.com/cloud/crowdstrike-launches-$1-million-security-breach-warranty/d/d-id/1331972
- https://www.welivesecurity.com/2018/06/01/europol-eu-team-fight-dark-web

Wireshark Demo

Sniffers

Sniffers are pieces of software or hardware meant for intercepting, analyzing, and interacting with network traffic

Examples:

- Wireshark - All around packet capture tool and capture analyzer
- Kismet - Sniffer meant for wireless sniffing
- Ettercap - Man in the middle attack sniffer
- Fiddler - Web traffic sniffer

Wireshark

- Excellent open-source sniffing tool
- Creates pcap and pcapng files, which contain captures of network traffic
- Industry standard
- Easy to start using, difficult to master
- Certification: WCNA
- Runs on both windows and linux

Limitations

- Wireshark lets you view raw packets and frames
- Wireshark is only able to capture the traffic that is visible in the subnet that the machine running it is in

Download the files found at the following link:

https://tinyurl.com/y7f6pj92

https://tinyurl.com/ybrajmga