

Cyber@UC Meeting 73

Basic Linux Distros

If You're New!

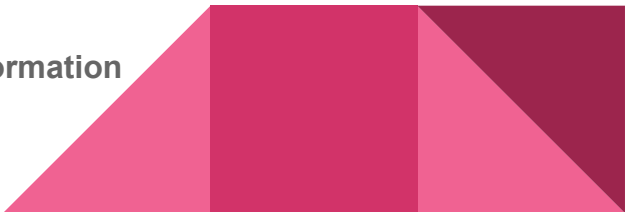
- Join our Slack: cyberatuc.slack.com
- Check out our website: cyberatuc.org
- **SIGN IN!** (*Slackbot will post the link in #general every Wed@6:30*)
- Feel free to get involved with one of our committees:
Content Finance Public Affairs Outreach Recruitment
- Ongoing work in our research lab!



Announcements

- **NSA Internship Application** window closing Oct 31st
- **NSA Codebreaker Challenge Event**
 - Saturday 10/20/18
 - Hosted by Cyber@UC
- **Chipotle fundraiser**
 - Saturday Nov 3rd 4pm–8pm
- **Election Nominations!**
- **Northrop Grumman check**
- **Cyber@UC Wiki now live!**
 - wiki.cyberatuc.org

Positions Up For Nomination:

- President
 - Vice President
 - Secretary
 - Treasurer
 - Head of Public Affairs
 - Head of Recruitment and Retention
 - Head of Outreach
 - Head of Content and Information
 - Head of Finance
- 

Weekly Content

WhatsApp Video Call Compromise

- Found by Project Zero
- Would allow a hacker to remotely take control of your WhatsApp by video calling through the app
- Memory heap overflow caused by malformed RTP packets in video call requests, causing corruption error and crashes the app
- Affected Android and iOS apps
- PoC published detailing steps on recreation of flaw
- Published PoC only causes crash, but real flaw exposes much more
- Only one of about 6+ major flaws I've covered in WhatsApp this year alone

LoJax UEFI rootkit by Sednit APT

- UEFI rootkits considered very dangerous because they are difficult to detect and can survive most security measures, like OS reinstall and hard disk replacement
- UEFI rootkits have been presented as PoC, others known to be used by government agencies
- First wild UEFI rootkit just found
- Sednit, is also known as APT28 or Fancy Bear:
 - DNC hack, TV5Monde hack, World Anti-Doping Agency email leak
- Called LoJax due to malicious use of LoJack anti-theft software
 - To protect itself against OS reinstall, implemented as UEFI module

Web Polluters: Xiongmai

- Since Mirai, in which Xiongmai was among the majority of infected devices, companies have been stepping up out of the box security
- Xiongmai has continually shown a preference for market share and price over any form of security improvements
 - Continue running devices on P2P network despite being advised against it
 - Warned by security researchers about flaws in their devices, but never made changes
 - Default username and password is admin, no password
- Several record breaking DDoS attacks have occurred since
 - Multiple security firms have listed Xiongmai's products as being major contributing factors
 - Ex. DVR remote login bypassed through forced browsing
- Xiongmai threatened to sue critics for defamation and promised to do a recall but never did either

Xiongmai (continued)

- 10s of millions of these weakly secured devices out there because Xiongmai controls 25% of the DVR market alone
- Survive through not selling to customers but getting rebranded by 3rd party companies rebranding Xiongmai products as their own
- Not driven/pressured to improve security
-



Recommended Reading

<https://thehackernews.com/2018/10/android-linux-kernel-cfi.html>

<https://thehackernews.com/2018/10/android-cloud-backup.html>

<https://thehackernews.com/2018/10/web-browser-tls-support.html>

<https://www.darkreading.com/operations/ibm-builds-soc-on-wheels-to-drive-cybersecurity-training/d/d-id/1333042>

<https://krebsonsecurity.com/2018/10/supply-chain-security-101-an-experts-view/>



Recommended Reading (continued)

<https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industry-notpetya/>

<https://www.darkreading.com/cloud/millions-of-voter-records-found-for-sale-on-the-dark-web/d/d-id/1333041>

<https://www.darkreading.com/endpoint/privacy/dod-travel-system-breach-exposed-data-of-30k-civilian-military-employees/d/d-id/1333036>

<https://thehackernews.com/2018/10/dark-web-drugs-kingpin.html>



Linux

What exactly is it?



The Topics Today Go Something Exactly Like This

- What is Linux
- What are distributions
- Benefits to different types of distro
- Remaining time spent showing off Kali tools

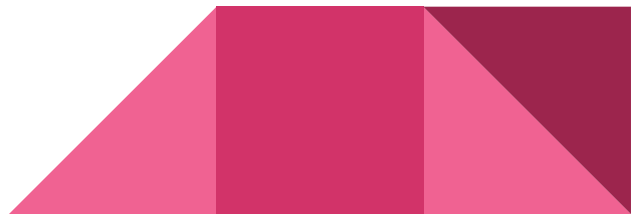
What is Linux

- Kernel developed in the early 90s
- Kernel acts as a bridge between applications and the actual data processing at the hardware level, manages system resources and communication
- What you think of as linux is actually an OS developed around that kernel
- Developed to be an open source alternative to Unix
- Linux is in basically every device that isn't a pc



How is it different from Windows and Mac

- Linux is free and open sourced
- Windows and Mac are more standardized into single versions
 - Linux is distributed into many distributions that are very different
- Linux and OS X are both Unix variants, but Windows is not, only unix similar
- Linux is dominant in terms on general computers, but Windows is dominant in personal/desktop computers




How is it different from Unix?

- Linux is a Unix-like OS
- Unix was developed by AT&T in late 60s to be a multi-tasking, multi-user os
- Written on C language allowing it to run on many hardware architectures
- Unix was not open source
- Linux was born in the early 90s to be a free open source alternative to unix
- For a user, there is little difference
- Unlike linux, Unix has several different versions of kernel



What are distributions and families?

- Linux Distribution: OS made from a software collection based on the Linux kernel and a package management system
 - Organized into major families by major distro and package manager
 - RPM: Red Hat, SUSE, CentOS, Fedora
 - Debian: Ubuntu, most other Linux OS
 - Pacman: Arch, Manjaro
 - Gentoo: Chromium
 - Slackware: Freenix, DNALinux, Linux From Scratch
 - Independent: Android
 - Primarily RPM and Debian
- 

Popular distros and their uses

Tried and True (normal/standard)

- Ubuntu: based on debian, tries to be more user/beginner friendly
- Debian: slower releases, broken into stable and unstable builds

- Fedora: frequent releases, less stable, but more up-to-date w/ new tech
- CentOS: more stable, but less frequent releases

- Arch: Less configured than other systems, helps with in-depth knowledge, fosters deep knowledge about your packages, for advanced users willing to see their stuff break all the time

Easy to Use

- Mint: works similarly to Windows
- Elementary: visually, very similar to Mac
- Ubuntu: does kind of fit between this category and the last



Serving a use case

- OpenBSD: security, considered one of if not the most secure os
- Kali: penetration testing and other similar tools
- Lubuntu: light weight, lots of distros work for this, like, soooo many





Put on your ~~3D glasses~~ **Linux Distro**
now

