Cyber@UC Meeting 52

BSides Recap and Memory Scanning

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

- BSides Cincy was AWESOME
- **We need to name our lab!**
- The Lab has been coming along great!
- **Dr. Sylvertooth** wants to talk to us! (**DHS Cybersecurity SME**)
  - https://www.linkedin.com/in/dr-randall-e-sylvertooth-55b35b47
- **UC Open House** for our **Lab and Cyber Range May 29th**
- Partnership with **Galois** in the works...still….

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

B-Sides Recap
Active Defense

Weekly Content

GLitch/Throwhammer

- Throwhammer is based off a well known exploit known as Rowhammer
- Rowhammer is vulnerability in dRAM where if a row is repeatedly accessed, the bits of an adjacent row are flipped
    - Used in many attacks to allow remote code execution
- Previous Rowhammer attacks have relied on privilege escalation
- Throwhammer bypasses this by sending malicious packets over LAN to cards with Remote Direct Memory Access (RDMA)
- Being a hardware vulnerability, there is no software patch that can really fix the issue

Google to Require Android Patching

- Google is taking steps to raise the security of all Android devices, not just the ones made by google
- Project Treble, revealed last year, re-architecting Android for easier updating and patching
- Oreo, the most recent version of Android is run on < 6% of devices
- Google is including patching into OEM agreements

Signal, not so secure

- Signal for Mac makes a copy of destructible messages in macOS notification center, where they can be recovered, even after self destructing
- Message remains in a user readable SQLite database
- Signal for Windows and Linux: Flaw in Signal, Electron framework, or both allowing for code injection
- Accidentally found while security researchers used Signal and one sent a vulnerable website with an XSS payload in its URL and the XSS executed on the Signal app
- A similar vulnerability where malicious HTML/JS can be sent as a message to steal messages as plaintext could potentially allow theft of Windows passwords too

Sources

RowHammer:

https://thehackernews.com/2018/05/rowhammer-attack-exploit.html
https://thehackernews.com/2016/10/root-android-phone-exploit.html

Android Security:

https://www.welivesecurity.com/2018/05/16/google-require-android-security-patches/
https://www.youtube.com/watch?v=r54roADX2MI
https://www.theverge.com/2018/4/12/17228510/android-phone-manufacturers-missed-security-updates-lie
https://twitter.com/secx13
https://developer.android.com/about/dashboards/

Signal:

https://thehackernews.com/2018/05/signal-secure-messaging.html
https://thehackernews.com/2018/05/signal-messenger-vulnerability.html
https://thehackernews.com/2018/05/signal-messenger-code-injection.html
https://thehackernews.com/2018/05/signal-desktop-hacking.html

RE1: Memory Scanner Basics

Someone put a pun here please

The Topics Today Go Something Exactly Like This

Topics:

- Memory Basics
- Why scan memory?
- What do Scanners do?
- Memory Scanners Available

Participation:

- Types of Scans (Exact, Range)
- Sequential Scans
- Editing

Memory Basics

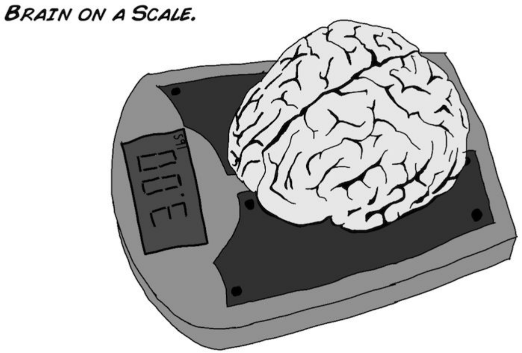
Only care about two properties of memory
{Address, Value}

Stack (Sequential)	Heap (Dynamic)	Pseudo Code
{ 0x01, 0xF1}		int a = 241
{ 0x02, 0xB2}	{0xB2, 0x09}	int *b = new int(9)

Here, the memory 0x01 could be a member variable where the memory at 0x02 could be a pointer to a heap value 0xB2

Why Scan Memory?

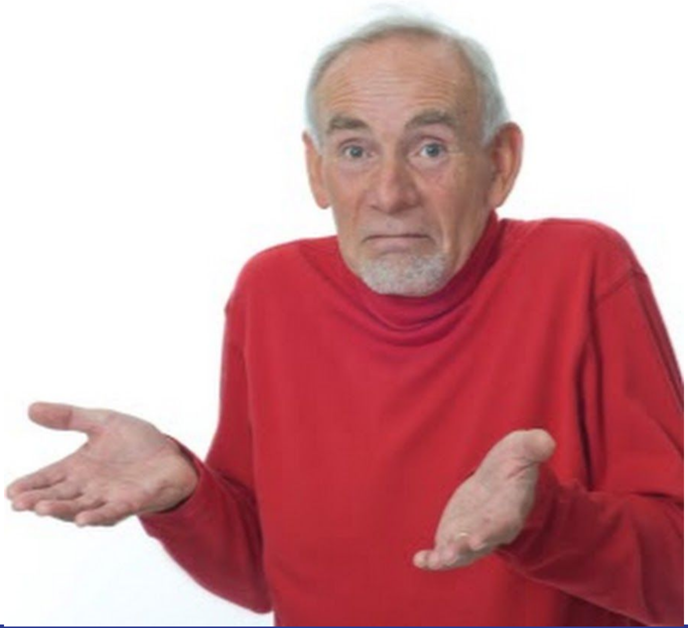
- Scanning memory can help find key values that you can intercept and react near instantly.
- We can write external programs to modify our target programs
- This can be the difference in a >0.20s human reaction and a <0.01s machine reaction



What do memory scanners do?

- Find certain values in a program’s memory (scanning)
  - Exact Value Scans
  - Value Range Scans
  - Incremental Scans
  - String Scans
- Edit values in a program’s memory (editing)
-

Linux not Required



Memory Scanners Available

Windows

- Cheat Engine
- Cheat Engine has extra stuff in it for publishing game hacks because that’s the target audience but we can still use it here

Linux/Mac

- scanmem (CLI)
- gameconqueror (scanmem UI)
- Both on Ubuntu apt repos

Let’s play around!

- Quick Demo on example_game_1.cpp
- Quick Demo on a real game without cheat detection built in