Hacker Curriculum

Adam Cecchetti
Leviathan Security Group

Who Am I?

- Adam Cecchetti
  - M.S. ECE Carnegie Mellon
  - B.S. CS Saint Vincent College
  - Leviathan Security Group
    - Principal Security Consultant
  - Amazon.com Security Team
    - Lead Engineer
  - Splitting Gemini, Nunchaku
  - Hacking Exposed 6th Ed

Who am I really?*

- 72.08 % Hacker
- 24.92% Engineer

* +/- 3.02% margin of error

What school taught me

- Mathematics
- Logic
- Programming
- Reasoning
- How to engineer a solution to a problem
- How to follow guide lines, rules, regulations, standards, and those silly laws of physics

What school also taught me.

97% is totally acceptable

What school didn’t teach me

- What “real” code / solutions look like
- What real deadlines look like
- What real code and soluations that comes from real dead lines looks like

What hacking has taught me…

- Engineers are incredibly talented people
- I make my living in that 3%
- **Everything** is broken
- Some things need nuked from orbit

The disconnect

- Engineering is a logical process
  - That involves making everything line up and work correctly even when they don't
  - Schools have gotten very very good at this part
- Hacking is a combination of many processes
  - Logical, creative, insight, perspective, and mindset
  - Less is often more
  - There is no spoon

Hacking

"Finding a creative way to make something function in a way it was never intended"

Teaching Hacking

- Tricks, Tools
- Prerequisites are high
- Mindset Mindset Mindset

Tricks and Tools

- Security courses spend a lot of time here
- Many current hacking classes
  - Tool X allows you to find Y
  - Use X tool to try and find Y
  - Take Y and try technique Z
  - When Z fails move on to A-J

A more concrete example

- Nmap is a network scanner that allows you to find open services and ports
- Scan your network to find open ports
- Attempt to use an exploit on these services
- If the exploit does not work try another service

Prerequisites are high

- Standard engagement involves knowledge of
  - 1-2 Languages 1 CPU Architecture
  - 1 Operating System or Application container
    - Windows, IE/Firefox
  - Networking - 1 Protocol
  - Data storage - File or Database
  - Debugging, Scripting
  - Standard Domain exploits

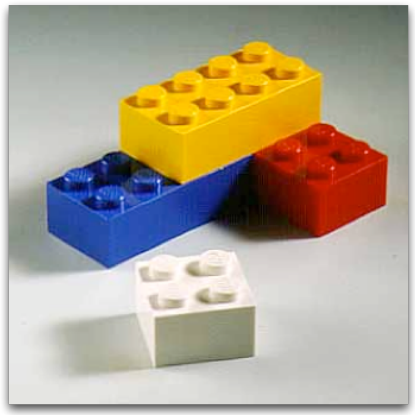
Prerequisites are high

Difficult Engagement

- 2-5 languages 1-3 CPU architectures
- Multiple Operating Systems / App Containers
- Networking : 1-10 protocols
- Hardware : Drivers, IOCTLs, Timing
- Multi Domain Exploits
- Nearly Full Insight
  - Debugging, reversing, proxies calls, scripting
  - A lot of scrolling text…

Mindsets

- Engineering mindsets
  - Start in a constrained environment
  - This block will not move thus I can build something on the block



- Hacking mindsets
  - Start in a unconstrained environment
  - Can I move the block? No?
  - Can I move the thing under the block?
  - And so on…

Is it really that hard to teach mindset?

The Coffee Shop Talk

^Abridged

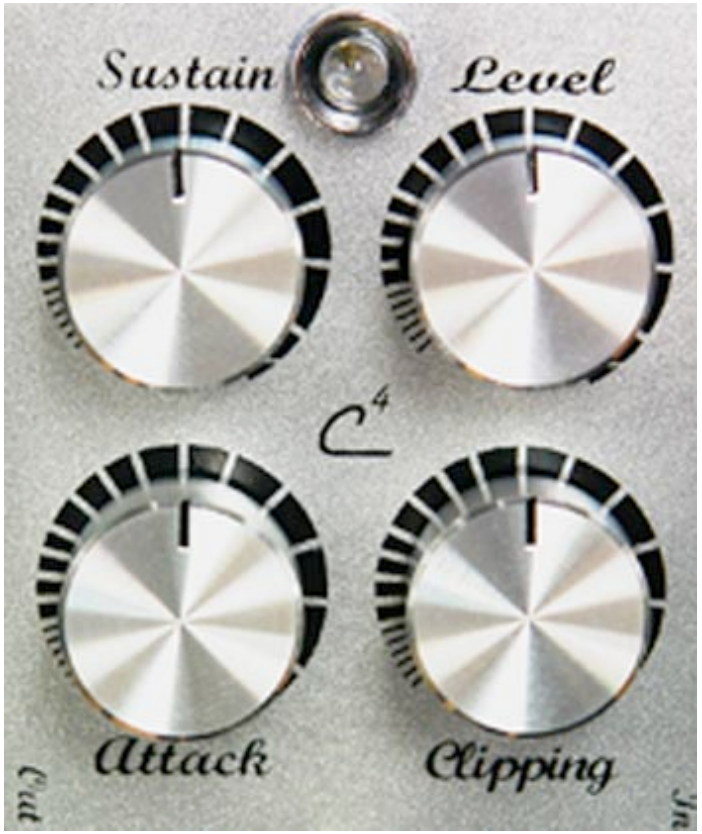
Hacker Mindset

- The knobs – Free your mind
- The chest– Malicious Mindset
- Pirate – Trust
- Lines – Breaking The Rules
- Toll Road – Breaking More Than One Rule

What schools teach

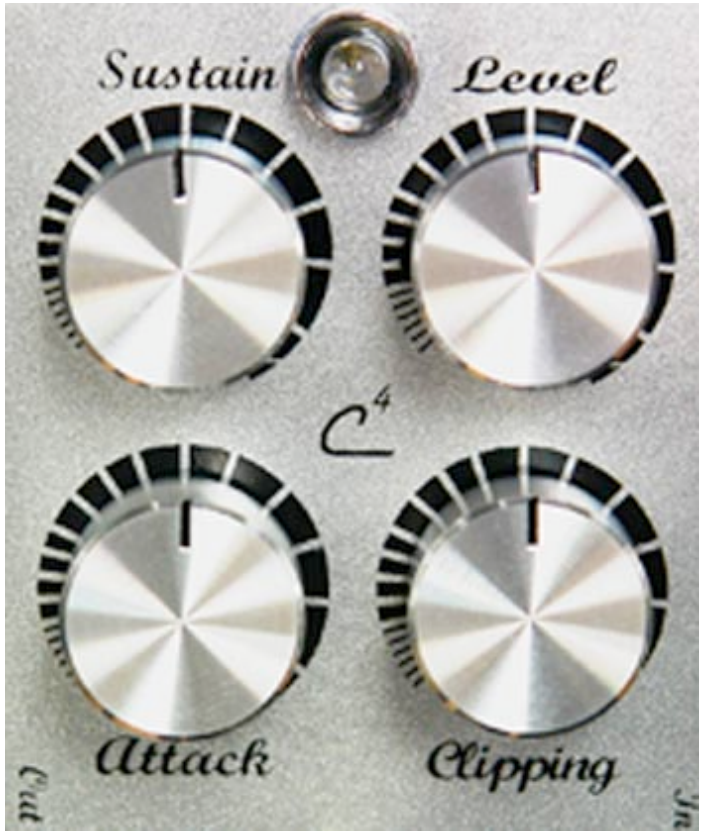
- The 4 knobs turn and stop at 1 to 10
- One knob controls Sustain
- One knob controls Level
- Clipping no longer works
- Don’t turn the attack knob
- The light will blink when

your neighbors think the volume is too loud



What hackers teach

- Make the knobs blink.



The Chest

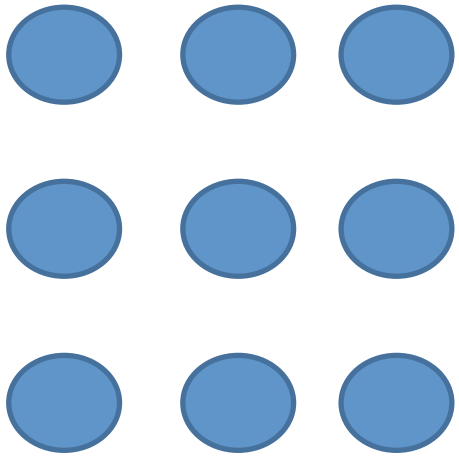
The Pirate

On the next slide is a picture of one pirate

A Pirate

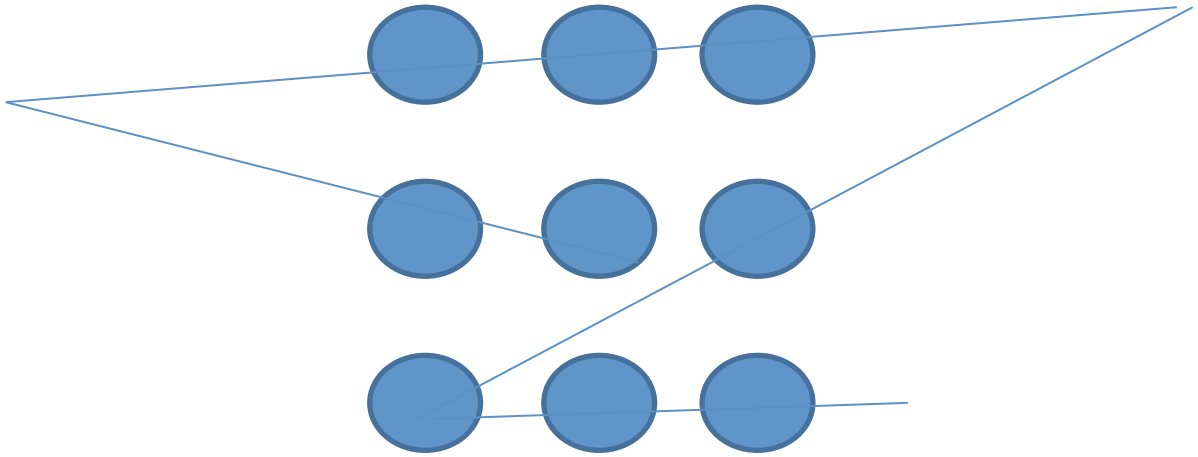
Dots

Connect the following dots with 4 lines without lifting your pen.



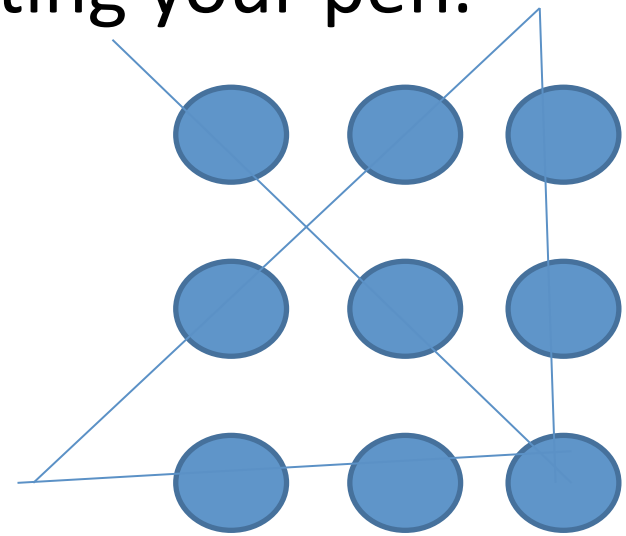
Dots

Connect the following dots with 4 lines without lifting your pen.



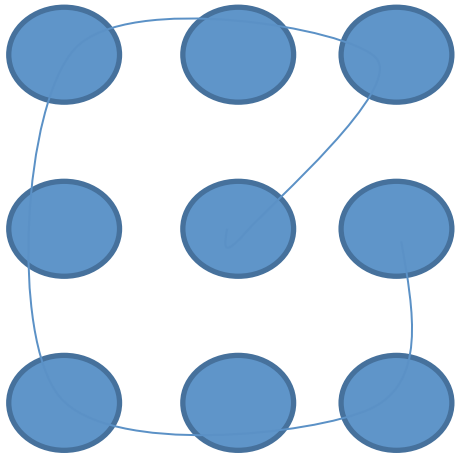
Dots

Connect the following dots with 4 lines without lifting your pen.



Dots

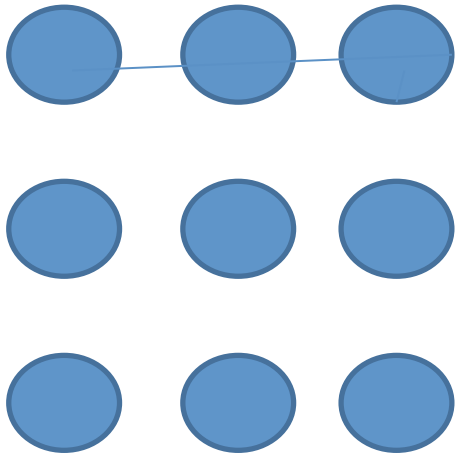
Connect the following dots with 4 lines without lifting your pen.



You must use straight lines.

Dots

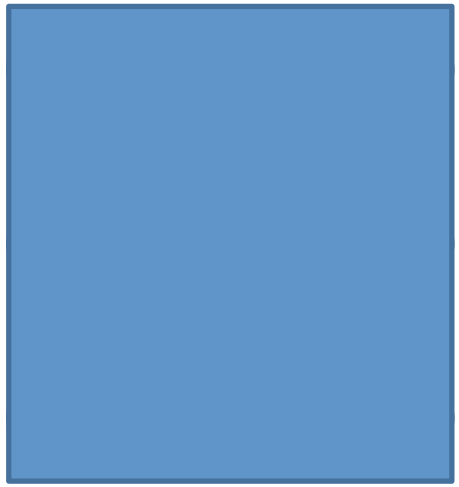
Connect the following dots with 4 lines



How many dots?

Dots

Connect the following dots with 4 lines



What dots?

The Gate

The Gate

Cars drive on roads

The gate requires a access card

The access card is only granted to …

Teaching hacking

- 15 % tools
- 15 % very wide domain knowledge
- 70 % mindset