Hacker Mindset

Batman's Kitchen Meeting 1

Krishna Bhat

Housekeeping

- Wednesday: beginner friendly talks, some guests
- Fridays: special topics talks, Capture The Flag competitions
- This friday join us to look at interesting things on UW's network!
- Join our discord: https://discord.gg/BV62RPKN

Intro

Why Teach Hacking?

- When used **ethically and responsibly** hacking is an important skill set
- Everything we teach is used by real cybersecurity professionals every day
- The best way to stop evil hackers is to find the vulnerabilities first
- Hacking is super fun

What Is A Hacker?

What Is A Hacker?

- Someone who exploits the gap between **assumptions** and **reality**
- Not just computer systems
  - Social systems
  - Physical security systems
  - Public information systems

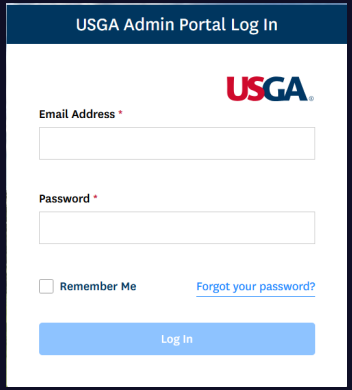
How Does A Hacker Think?

- Interest in invisible systems
- Learn how systems work and don't work
- Willing to go down rabbit holes

Part 1: Hack The Internet

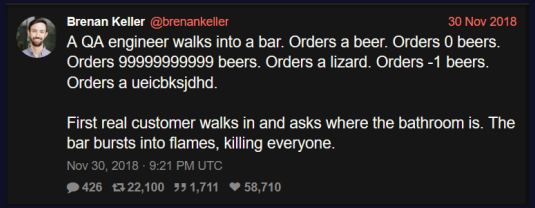
Case Study - Admin Login

- Things a hacker might try:
  - “admin / password” or “admin / admin”
  - Weird Characters
    (`:;_-=**&^!#$%[⠿-⠉⠿]▄⤸⤵-⤶-◦Ⓗ✻⏻⥤↩⤮⌯⌬⌀ ⊸⩔⬇)
  - Usernames without passwords
  - Submitting passwords from a data breach
  - Forgor password 💀



Case Study - Shopping Application

- What a hacker might try on a shopping website:
  - Intercept web request and submit a negative price
  - Edit a coupon code to be 100% off
  - Submit a refund for something you didn't buy
  - Try to buy 1000000000 of an item. Try to buy -1 of an item
  - Mess with other people's carts
  - Brute force coupon codes



Case Study - UW Network

- Did you know you can scan **every publicly visible device on UW's network** in seconds?
  - https://www.shodan.io/search?query=org%3A%22University+of+Washington%22
  - http.html:"admin"
  - http.html:"camera"
  - http.html:"index of"
- Did you know you can find **every UW website** in seconds?
  - https://crt.sh/?q=washington.edu&exclude=expired&group=none
  - https://ui.ctsearch.entrust.com/ui/ctsearchui

Part 2: Hack The People

Humans Are The Weakest Link

- People make mistakes and assumptions
- It's easier to log in and than hack in
- You don't need a PhD in cryptography to guess someone's Draftkings password is *2019Champs!*
- You can just ask nicely and they will give you sensitive information
- **Social Engineering** is an entire field of security

Case Study - Shopping App 2

- In 2012, Amazon let you:
  - Reset your Amazon password by providing an associated credit card
  - Add a credit card to an Amazon account with a call to customer support
  - Hack any Amazon account
- The Plan:
  - Add a credit card to a victim account (use a stolen one for more anonymity)
  - Use the new credit card number to reset their password
  - Profit

Skills required: being able to call a customer support (impossible for gen z)

Case Study - Shopping App 2

- How does the approach change in this example
- When dealing with human elements
  - Nondeterministic
  - Need to be good at talking, not just writing code
  - more connected to the 'real world'

Case Study - Office Building

How real world can we go?

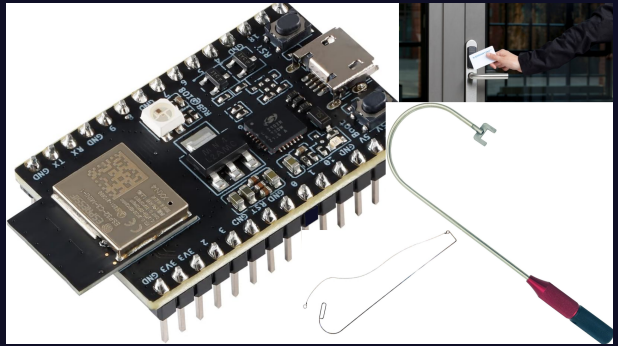
- What if you want to break into Amazon HQ?
- Walk in behind someone

What if they check your badge?

- Clone an employee's badge at their favorite coffee shop
- Pretend to be someone who does not need a badge
  - Elevator repair tech
  - DoorDash delivery driver
  - Building inspector

Case Study - Office Building

- What if we want something higher tech?



Part 3: Hack The Planet

Case Study - Transit

No one knows how transit cards work

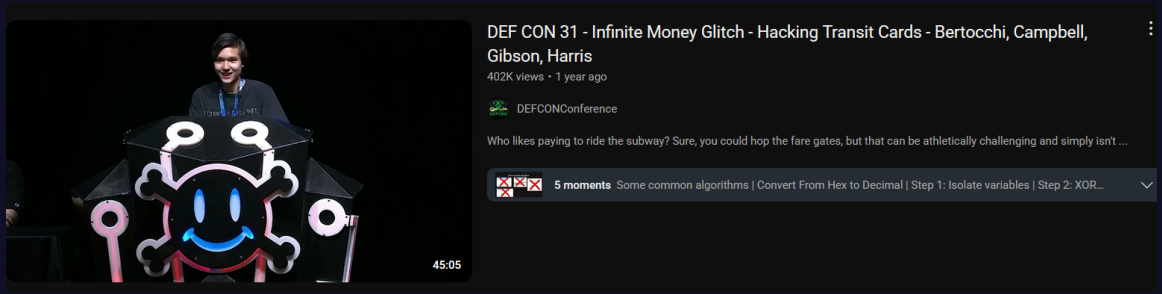
Case Study - Transit

'No one knows how transit cards work' is what transit orgs think

- If you know how they work you can break their encryption and change them
- Add as much money as you want or set yourself to be an employee with free rides
- Some don't even use encryption!

Case Study - Transit

- https://medium.com/@bobbyrsec/operation-charlie-hacking-the-mbta-charliecard-from-2008-to-present-24ea9f0aaa38

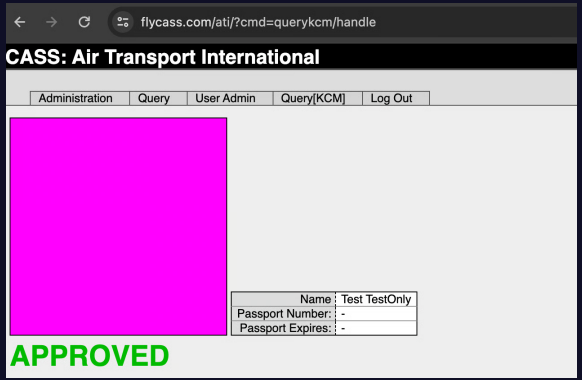


Case Study - Airport

- Last year security researchers gained complete control over the TSA's Known Crewmember Database
- They could skip TSA lines and enter airline cockpits
- The technique is so simple we're teaching it to you next week
- The vulnerability was around for years before someone checked

Case Study - Airport

- https://ian.sh/tsa

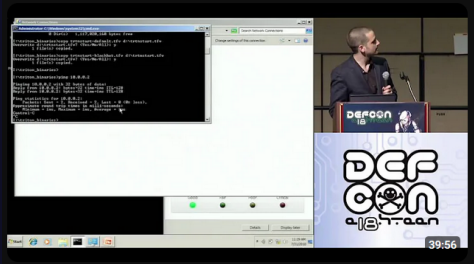


Other Cool Hacks

Hacking Millions of Modems (and Investigating Who Hacked My Modem)

Mon Jun 03 2024

Other Cool Hacks



DEF CON 18 - Barnaby Jack - Jackpotting Automated Teller Machines Redux

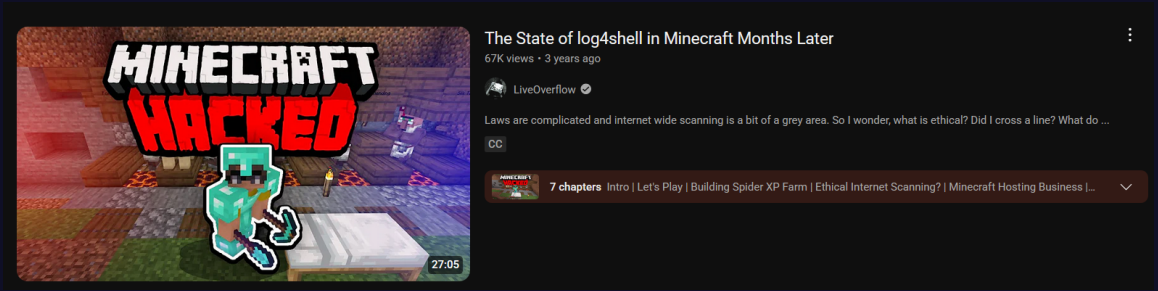
92K views • 11 years ago

DEFCONConference

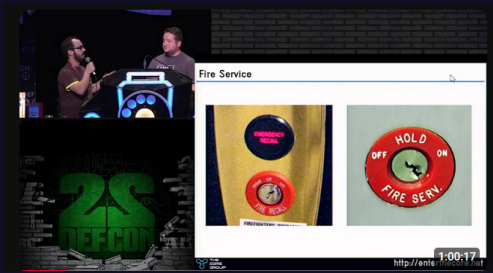
Barnaby Jack - Jackpotting Automated Teller Machines Redux The presentation "Jackpotting Automated Teller Machines" was ...

21 chapters Intro | Goal | Current Attacks | Standalone ATMs | Retail ATMs | Security hurdles | Getting a show |...

Other Cool Hacks



Other Cool Hacks



DEF CON 22 - Deviant Ollam & Howard Payne - Elevator Hacking - From the Pit to the Penthouse

828K views • 10 years ago

DEFCONConference

Elevator Hacking - From the Pit to the Penthouse Deviant Ollam The CORE Group Howard Payne The CORE Group Throughout ...

CC

With Great Power

- Ethical hacking is not just about following the law
- To hack ethically you must understand the impact of technology on people
- It is our job as hackers to fight for
  - The security of people's data
  - People's right to privacy
  - A fair and equitable internet

- All of these are actively being eroded by corporations, governments, and freaks

tl;dw

- Hacking is not about green code in a terminal
- Hacking is looking at how systems are designed, used, and abused
- Anyone can be a hacker if they think like one
  - Pay attention to the systems around you
  - Explore rabbit holes
  - Challenge assumptions
  - "Take chances, make mistakes, and get messy" - Ms. Fr1zzl3

What Do You Want to Hack?