

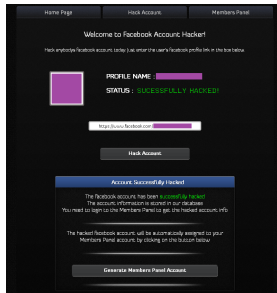
Learning How to Hack!

GDSC EAEAT

Yusuf Hegazy

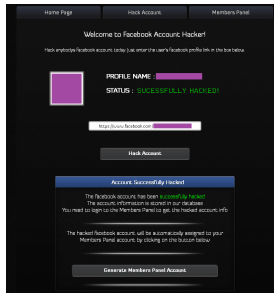
What is Hacking?

- Hacking a Facebook Account?



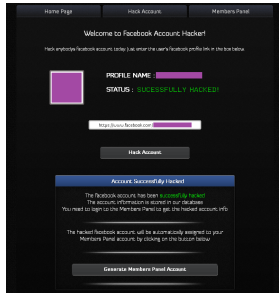
What is Hacking?

- Hacking a Facebook Account?
- Hacking Mobile Phones?



What is Hacking?

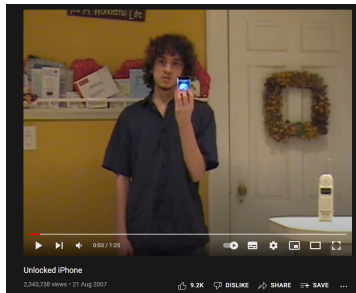
- Hacking a Facebook Account?
- Hacking Mobile Phones?
- Hacking Computer Games?



"A hacker is a person skilled with computers who uses their technical knowledge to overcome an obstacle"

Famous Hackers: George Hotz

- First Jailbroken iPhone - 2007



Famous Hackers: George Hotz

- First Jailbroken iPhone - 2007
- First Jailbroken PS3 - 2010



Famous Hackers: George Hotz

- First Jailbroken iPhone - 2007
- First Jailbroken PS3 - 2010
- Worked at Google Project Zero

Famous Hackers: George Hotz

- First Jailbroken iPhone - 2007
- First Jailbroken PS3 - 2010
- Worked at Google Project Zero
- Got offer from Elon Musk

Famous Hackers: George Hotz

- First Jailbroken iPhone - 2007
- First Jailbroken PS3 - 2010
- Worked at Google Project Zero
- Got offer from Elon Musk
- Started Comma.ai



Cyber Security: The Science of Hacking

Application Security

Web Security

- HTTP Protocol

Web Security

- HTTP Protocol
- HTML, CSS

Web Security

- HTTP Protocol
- HTML, CSS
- Javascript, PHP

Web Security

- HTTP Protocol
- HTML, CSS
- Javascript, PHP
- Python, Go, Rust and more!

Web Security

What exactly do we do?

- Analysis -> Hypothesis

Web Security

What exactly do we do?

- Analysis -> Hypothesis
- Test for different exploits

Web Security

What exactly do we do?

- Analysis -> Hypothesis
- Test for different exploits
- Build a methodology

Forensics

- Logs

Forensics

- Logs
- Network Traffic

Forensics

- Logs
- Network Traffic
- Memory Dumps

Reverse Engineering

- Computer Architecture

Reverse Engineering

- Computer Architecture
- Assembly Language

Reverse Engineering

- Computer Architecture
- Assembly Language
- C/C++

Reverse Engineering

- Computer Architecture
- Assembly Language
- C/C++
- Debuggers/Disassemblers/Decompilers

Exploitation

- Solid understanding of Memory

Exploitation

- Solid understanding of Memory
- Reverse Engineering

Exploitation

- Solid understanding of Memory
- Reverse Engineering
- Writing Exploits in C/Python

Hardware Security

- JTAG

Hardware Security

- JTAG
- Communication Protocols

Hardware Security

- JTAG
- Communication Protocols
- RF

Hardware Security

- JTAG
- Communication Protocols
- RF
- Dumping Firmware

Cybersecurity Jobs

- Red Team
- Blue Team
- Purple Team

Red Team

- Penetration Testing
 - Web
 - Mobile
 - Network
 - Hardware

Blue Team

- Threat Hunting
- Digital Forensics
- Incident Response
- Security Operations Center

There's even more...

- Malware Analysis
- Vulnerability Research
- Exploit Development
- GRC
- DevSecOps

Getting Started with Cybersecurity

Skills Involved - Getting Started

- Linux
- Scripting
 - Python
 - Bash
 - Powershell
- Little Networking

Skills Involved - Advanced

- Computer Architecture
- Cryptography
- Low-Level Programming
- Reverse Engineering
- Networking

CTFs

CTFs

- Goal is to solve a challenge and get the flag
- Helps you apply what you learn
- A lot of fun

CTFs: Categories

- Web
- OSINT
- Forensics
- Exploitation
- Reverse Engineering/Malware Analysis
- Networking
- Cryptography
- Hardware

CTFs: Starting Point

- PicoCTF
- OverTheWire
- TryHackMe

Tips

Tips

- 1 Apply what you learn

Tips

- ❶ Apply what you learn
- ❷ Learn to Google!

Tips

- ❶ Apply what you learn
- ❷ Learn to Google!
- ❸ Take notes

Tips

- ❶ Apply what you learn
- ❷ Learn to Google!
- ❸ Take notes
- ❹ Find a mentor

Tips

- ❶ Apply what you learn
- ❷ Learn to Google!
- ❸ Take notes
- ❹ Find a mentor
- ❺ Blog your research

Tips

- ❶ Apply what you learn
- ❷ Learn to Google!
- ❸ Take notes
- ❹ Find a mentor
- ❺ Blog your research
- ❻ Create a Twitter account

Common Pitfalls

Common Pitfalls

- 1 Our minds don't work the same

Common Pitfalls

- ❶ Our minds don't work the same
- ❷ Don't ask to ask, just ask

Common Pitfalls

- ❶ Our minds don't work the same
- ❷ Don't ask to ask, just ask
- ❸ The XY Problem

Don't ask to ask



Don't ask to ask



Great Resources

- Cybersecurity Introduction - Nakerah Network
- The Nakerah Podcast
- So you wanna do security?
- Technology Essentials