Teaching Hacking

• Is it ethical to teaching hacking skills in a university?
• Does this teach necessary skills for defenders?
• Does it teach skills only necessary for attackers?
• Should such courses have an ethics unit?
Hack-Back

• By whom? Governments? Victims? Vendors? Vigilantes?

• What is an acceptable goal?
  • Botnet takeover for neutralization?
  • Disinfect machines?
  • Gather evidence?
  • Deter attackers?

• What if attribution isn’t certain? What if innocent victims’ computers are used to launch the attack?
Vulnerability Disclosure

• Should researchers disclose vulnerabilities publicly? Should they wait a few months, to let patches be developed and deployed?

• Does it help defenders look for indications of compromise?

• Or does it teach attackers what to do?

• Should “bug bounty” programs, where vendors reward researchers who find holes, include non-disclosure agreements (NDAs)?
Monitoring

• Is it proper to monitor other people’s Internet traffic and computer use to see if they’ve been hacked?
  • What about just the metadata and not the content?

• Who should be allowed to do this? Governments? ISPs? Employers? Software vendors?

• If consent is sought, would it really be voluntary?