Offense vs. Defense

Arshiya Khan

Ph.D. Candidate, ECE

University of Delaware, USA

Agenda

- Cybersecurity
- Cyber Threats
- Phishing Attack
- Wireshark
- System Hardening

Cyber Security

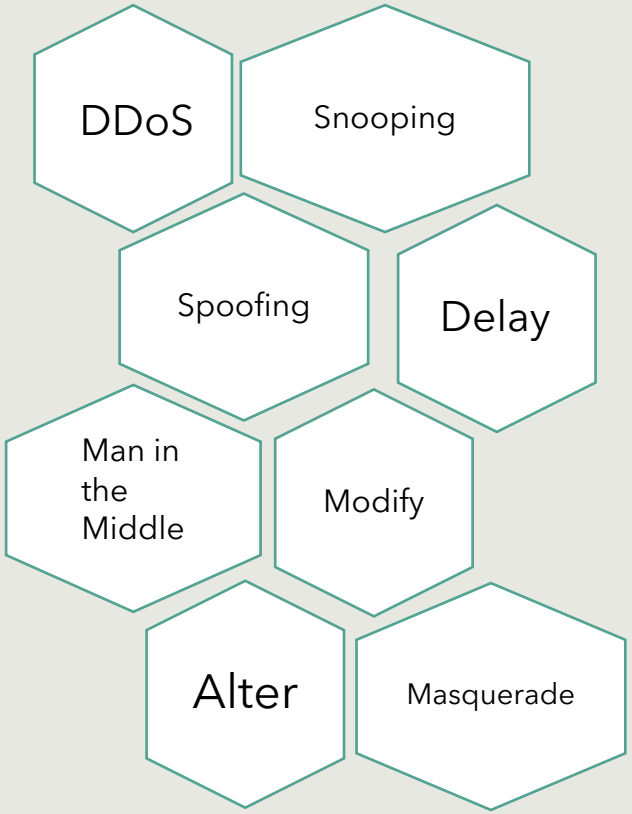
- Computer and Network Security
- Preserve CIA
  - Confidentiality
  - Integrity
  - Availability
- C? I? or A?
  - Credit card numbers are stolen
  - Car
    - Broken
    - Stolen

Cyber Security

- C? I? or A?
  - A user has gained root privileges on an E-commerce website. Changed the domain name of the website. Put all items on 50% discount.

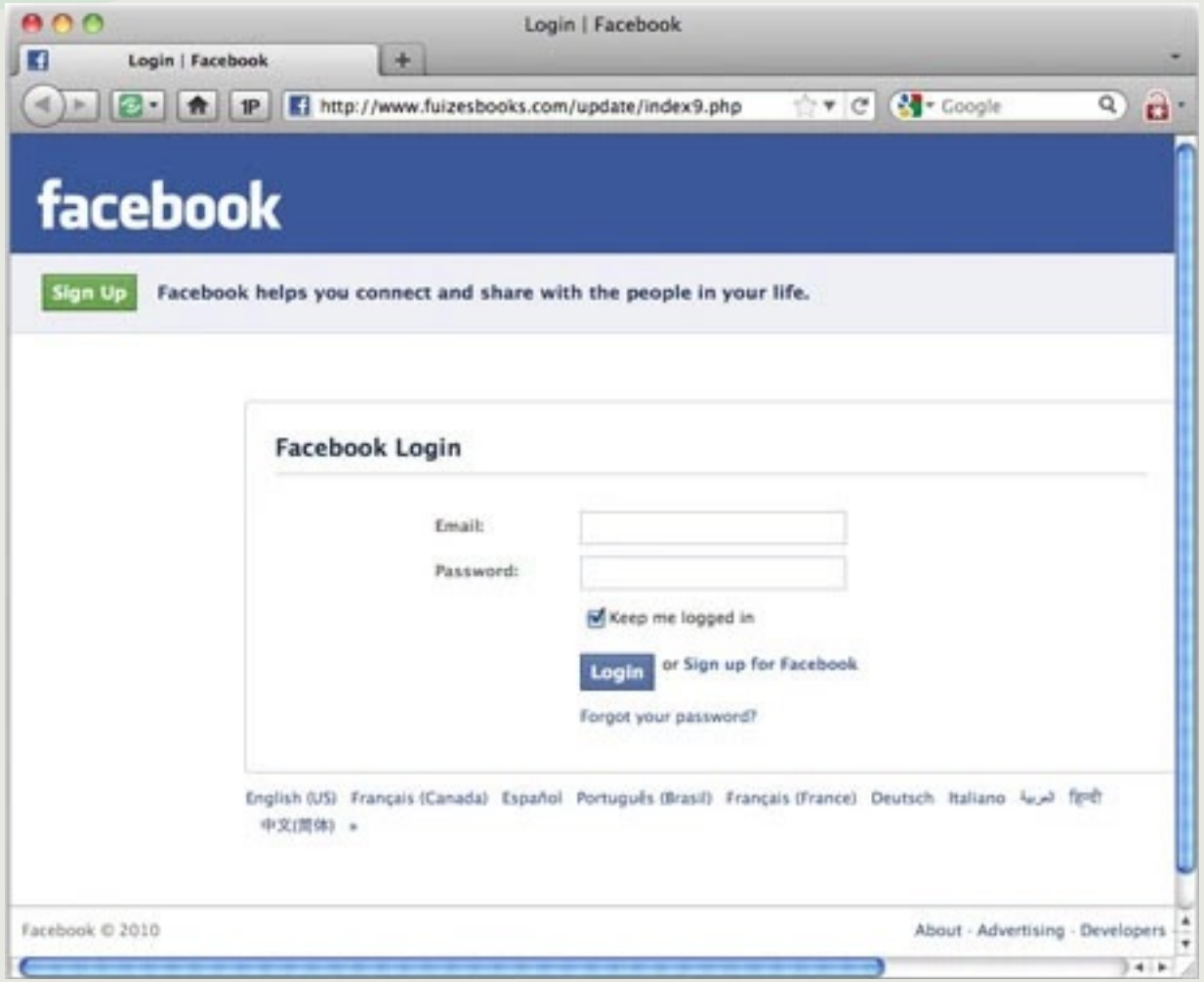
Cyber Threats

- Potential Violation of CIA
- Classes:
  - Disclosure – Unauthorized access to information
  - Deception – Acceptance of false data
  - Disruption – Interruption or prevention of correct operation
  - Usurpation – Unauthorized control of some part of a system
- SQL Injection Attack
  - Try it!
  - Classify?



Phishing Attack

- Social Engineering technique
- Collection of personal data carried out illegally or fraudulently through the internet
- Use the information collected to make purchases online, bank transfers or cash withdrawals on behalf of the fraud victim
- Examples


Login | Facebook
Login | Facebook
http://www.fuizesbooks.com/update/index9.php
Google
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
Facebook Login
Email:
Password:
Keep me logged in
Login
or Sign up for Facebook
Forgot your password?
English (US) Français (Canada) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी
中文(简体) »
Facebook © 2010
About · Advertising · Developers


Log in | Facebook
Log in | Facebook
facebook.com
https://www.facebook.com/login.php
Google
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
Facebook Login
Email address:
Password:
Keep me logged in
Set Facebook as my home page
Log in
or Sign up for Facebook
Forgotten your password?
English (UK) English (US) Cymraeg Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी »
Facebook © 2011
Mobile · Find friends · Badges · People · Pages · About · Advertising · Create a Page · Developers

Wireshark

- Network Packet Analysis
- Install software https://www.wireshark.org/
- Examine http://mailtranscripts.com/

System Hardening

- Defensive policies and steps to make your system difficult to hack
- Computer Hardening
- Network Hardening
- https://www.thefanclub.co.za/how-to/how-secure-ubuntu-1604-lts-server-part-1-basics

Thank You!