Quick Announcements

• Midterms will be returned today (after class)
  – Check rubric online!
• Privacy lecture merged with DDOS class
• CTF1 ends today (scoring script just stopped)
  – Report: 1-2 pages:
    • Describe strategy for each team
    • Discuss results, what worked/didn’t work, any obstacles, etc.
    • Have 1 section describing team roles
    • Each member must print and submit their own report in class with their own section listing their contributions made to the team effort
      – Or submit via e-mail with everyone CC’d
    • Due 4/4 (but submit sooner while it’s still fresh in your head)

• CTF2 Phase 0 starts today
  – Get with your groups now
Introduction to Security

Luis Garcia
USC CSCI 430

CTF 1 Debrief +
CTF 2 Overview
Each red and blue team:
- What was your strategy?
- What did you try?
- What worked/didn’t work?
- Any obstacles?
CTF2: Password Design and Cracking

- We’re going to practice designing password policies and cracking them
- All members will work together on all tasks
- CTF2 is broken down into 3 phases
CTF2: 3 Phases

• Phase 0: Web Server + password policy design
  – 3/28 – 4/11
  – Develop web server and have users create accounts + passwords
• Phase 1: Logging in activity
  – 4/11 - 4/18
  – Generate log in activity for a week, including password resets
• Phase 2: Password Cracking
  – 4/18 – 4/25
  – Each team will be given other teams’ password hashes and you’ll try to crack them
CTF2 Phase 0: Web Server + Password Policy Design

• Goal of each team
  – Develop web server for accepting accounts from students in class
  – Develop password policy to help users create strong and memorable passwords
    • If policy is too strict, users will forget
    • Reject passwords that do not follow it
CTF2 Phase 0: Web Server + Password Policy Design

- Create a web site that allows users to register and log in with USC username
  - just the part before @ sign, e.g., my username would be luisga
  - Any student in the class should be able to register and later to log in
  - Students should NOT use any previously used password from their personal accounts
- pass the parameters via "GET" method between the forms so that we can easily extract statistics about how often each student attempted to log in. If a user logs in successfully, they should be redirected to a Web page called "success.**" Otherwise, they should be redirected to a Web page called "failure.*".
- You can display whatever content you want on "success.*". On the other hand "failure.*" should have links to login page to let user try again and a link where a user can click to receive a reset email. The reset email (sent to the username the user has provided) should let the user click on it and then be taken to a reset page called "reset.*", where they can set their password again.
  - On the other hand "failure.*" should have links to login page to let user try again and a link where a user can click to receive a reset email. The reset email (sent to the username the user has provided) should let the user click on it and then be taken to a reset page called "reset.*", where they can set their password again.
CTF2 Phase 0:  
Web Server + Password Policy Design

- Teams' Web servers run on Amazon EC2 (Ubuntu 22.04) at the following IP Addresses:
  - Team 1: 18.188.162.148
  - Team 2: 3.145.9.225
  - Team 3: 3.144.113.23
  - Team 4: 3.133.129.167
  - Team 5: 3.15.235.208

- You can access your webserver via ssh:
  - ssh –i ctf2teamX.pem ubuntu@ip
  - The .pem files are located in /groups/USC430/team_144_X/ctf2teamX.pem, where “X” is replaced with your team number.
  - Copy the .pem file to your local computer and type
    - chmod 400 ctf2teamX.pem
    - Ensures private key is protected
CTF2 Phase 0:
Web Server Requirements

• Install any web server you like (you can reuse from CTF1)
• Password stored at the web server must be stored as an MD5 hash—with or without salt
• Do not store passwords in clear text in your database
  – You may want to store some encrypted version of passwords somewhere on the server so that you can decrypt them and see the plaintext
  • Useful if you try to crack each user’s passwords on the other servers, if the user reused or versioned their password
CTF2 Phase 0: Password Policy Ideas

• Survey: each member should talk to 5 different people (e.g., close friends, family members, etc.)
  – Survey their best password creation strategies for creating strong and memorable passwords

• Survey password policies from various big websites

• Team members should use this input to brainstorm best password policy design
CTF2 Phase 0: Suggested Division of Work

• All members work on survey
• Rest of the work:
  – Some students work on web server setup and installation
  – Some work on password policy definition (initial definition and revise based on early success/failure measures from your own team members)
  – Rest can work on web functionality (writing web pages, setting up database, etc.)
• To begin, design a simple login page that takes you to “success.*” and “failure.*” and stores the passwords
  – You can then extend this in parallel with other tasks
• E-mail sending task is tough because EC2 machines can’t send email directly
  – Start that task early and dedicate one team member to this
  – Make sure they deliver
  – Guidelines on Gmail email provided in link on CTF2 page
CTF2 Phase 1: Logging In

- After each team completes the webserver design, all students are required to log into each web server at least twice a day
- Revisit the page and click on links showed in overview part for each team
- Reset password if you forgot it
- Logging in activity will become 30% of your grade on this competition
- Set a reminder at the same time each day
CTF Phase 2: Password Cracking

• Each team will be given all other teams’ password hashes
  – Includes any salts if they are used
  – They should also provide password policy

• You can download any password cracking tools from the internet
  – John the Ripper: http://www.openwall.com/john/
  – Hashcat: https://hashcat.net/hashcat/
CTF Phase 2: Suggested Division of Work

• Entire team should work on password cracking
• Each member can choose a tool to use and crack independently
• Try to diversify here
• Some members may want to try manual cracking
  – Use plaintext passwords that users used on your server and try them and their variations on other servers
CTF2 Scoring

A team's score will be calculated as \( T + S/(S+F) - R/L - C/A \), where:

1. \( T = 1 \) if their server was ready on time (end of class on 4/11), 0 otherwise
2. \( S \) is the number of successful logins in the part 1
3. \( F \) is the number of failed logins in the part 1
4. \( L \) is the number of attempted logins in the part 1 = \( S + F \)
5. \( R \) is the number of password resets
6. \( C \) is the number of passwords that the other teams cracked for this server.
7. \( A \) is the total number of password hashes
CTF2: Exercise Dynamics

• All server code will be frozen on 4/11
• Logging in activity from 4/11-4/18
• Cracking happens after 4/18
Final Grading

• Will be graded based on the contribution to the team effort, not based on team’s performance
• A similar reporting system will be used—where everyone needs to sign off on
• Grades assigned as follows:
  – 4 points for participation in design and dev
  – 3 points for participation during cracking
  – 3 points for login activity