CSE 127 Discussion Week 9

Ariana Mirian, Zoom
This is being recorded.
Overview of Today

• PA5 overview
• User Authentication
• Malware
• Open Office hours
PA5

• Currently released – should have received an email tar
• Due June 4\textsuperscript{th} at 12:30 PM Pacific
  • Or June 11\textsuperscript{th} 12:30 PM HARD DEADLINE
• You need to get Stefan’s “token”
  • Fake token; everything is constrained on the server(s)
• Linux commands that may be helpful
  • nc, nmap, tcpdump, wget
• Three assignments on Gradescope
  • “Transcript” hint while you work through the steps
  • “Token” is token
  • Writeup is list of steps that you took
PA5

• At every point in the project ask yourself:
  • How can I find information that “hidden”?  
    • Concealed, but still discoverable

• How to think like a hacker
  • Some of the steps take time
  • Might be “patterns” that are useful in your steps
User Authentication Overview
Three types of authentication factors

- Something you know
- Something you have
- Something you are

- Why do we have multiple types of authentication? How do they help?
Something you know

- Passwords!
  - Where are the points that an attacker can get the password?
Something you know

• Passwords!
  • Where are the points that an attacker can get the password?
  • How would these motivating factors changed based on individual scenarios?
Something you know

• Passwords!
  • Where are the points that an attacker can get the password?
  • How would these motivating factors changed based on individual scenarios?

• Physical access to user
Something you know

• Passwords!
  • Where are the points that an attacker can get the password?
  • How would these motivating factors changed based on individual scenarios?
• Physical access to user
• Physical access to user machine
Something you know

• Passwords!
  • Where are the points that an attacker can get the password?
  • How would these motivating factors changed based on individual scenarios?
• Physical access to user
• Physical access to user machine
• In transit -- Phishing
  • Get the password by tricking the user
Something you know

• Passwords!
  • Where are the points that an attacker can get the password?
  • How would these motivating factors changed based on individual scenarios?

• Physical access to user

• Physical access to user machine

• In transit -- Phishing
  • Get the password by tricking the user

• Data leaks/dumps
  • This is where reusing passwords becomes a problem
  • Plaintext password is worse than hashed password is worse than fast salted password is worse than slow salted password
Something you have

- Cards, password tokens (one time on physical and electronics), USB/NFC tokens
- What are the strengths and weaknesses of these various approaches?
Something you are

- Biometrics!
- We’re all unique enough, right?
- Problems with biometrics:
  - Spoofable (still!)
  - Perhaps not as accurate
  - Doesn’t scale well
Malware Overview
Overview of malware

• Difference between virus and worms
  • Virus driven to attach to new program by human action
  • Worm driven to attach to new host; self spreading
Overview of malware

• Difference between virus and worms
  • Virus driven to attach to new program by human action
  • Worm driven to attach to new host; self spreading

• Different types of viruses
  • Bootstrap, Memory Resident, Encrypted, polymorphic/metamorphic
Overview of malware

• Difference between virus and worms
  • Virus driven to attach to new program by human action
  • Worm driven to attach to new host; self spreading

• Different types of viruses
  • Bootstrap, Memory Resident, Encrypted, polymorphic/metamorphic

• Scanning for viruses
  • Look for their “signatures”
Overview of malware

• Difference between virus and worms
  • Virus driven to attach to new program by human action
  • Worm driven to attach to new host; self spreading

• Different types of viruses
  • Bootstrap, Memory Resident, Encrypted, polymorphic/metamorphic

• Scanning for viruses
  • Look for their “signatures”

• Detection mechanisms
  • Integrity check and Behavior detection
Open Office Hours